Numéro du rôle : 6672
Arrêt n° 158/2021 du 18 novembre 2021

A R R Ê T

En cause : le recours en annulation de la loi du 1er septembre 2016 « portant modification de l'article 127 de la loi du 13 juin 2005 relative aux communications électroniques et de l'article 16/2 de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité », introduit par Patrick Van Assche et autres.

La Cour constitutionnelle,

composée des présidents L. Lavrysen et P. Nihoul, des juges J.-P. Moerman, T. Giet, R. Leysen, J. Moerman, M. Pâques, Y. Kherbache, T. Detienne et D. Pieters, et, conformément à l'article 60*bis* de la loi spéciale du 6 janvier 1989 sur la Cour constitutionnelle, du président émérite F. Daoût et de la juge émérite T. Merckx-Van Goey, assistée du greffier P.-Y. Dutilleux, présidée par le président L. Lavrysen,

après en avoir délibéré, rend l'arrêt suivant :

*

* *

I. *Objet du recours et procédure*

Par requête adressée à la Cour par lettre recommandée à la poste le 7 juin 2017 et parvenue au greffe le 8 juin 2017, un recours en annulation de la loi du 1er septembre 2016 « portant modification de l'article 127 de la loi du 13 juin 2005 relative aux communications électroniques et de l'article 16/2 de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité » (publiée au *Moniteur belge* du 7 décembre 2016) a été introduit par Patrick Van Assche, Christel Van Akeleyen et Karina De Hoog, assistés et représentés par Me D. Pattyn, avocat au barreau de Flandre occidentale.

Le Conseil des ministres, assisté et représenté par Me S. Depré, Me E. de Lophem et Me T. Wouters, avocats au barreau de Bruxelles, a introduit un mémoire, les parties requérantes ont introduit un mémoire en réponse et le Conseil des ministres a également introduit un mémoire en réplique.

Par ordonnance du 7 février 2018, la Cour, après avoir entendu les juges-rapporteurs A. Alen et J.-P. Moerman, a décidé que l'affaire était en état, qu'aucune audience ne serait tenue, à moins qu'une partie n'ait demandé, dans le délai de sept jours suivant la réception de la notification de cette ordonnance, à être entendue, et qu'en l'absence d'une telle demande, les débats seraient clos le 28 février 2018 et l'affaire mise en délibéré.

À la suite de la demande des parties requérantes à être entendues, la Cour, par ordonnance du 1er mars 2018, a fixé l'audience au 21 mars 2018.

Par ordonnance du 28 mars 2018, la Cour a reporté l'affaire à l'audience du 25 avril 2018.

À l'audience publique du 25 avril 2018 :

- ont comparu :

. Me D. Pattyn, pour les parties requérantes, et Patrick Van Assche, en personne;

. Me E. de Lophem, Me T. Wouters et Me G. Ryelandt, avocat au barreau de Bruxelles, *loco* Me S. Depré, pour le Conseil des ministres;

- le président A. Alen et le juge J.-P. Moerman ont fait rapport;

- les avocats précités ont été entendus;

- l'affaire a été mise en délibéré.

Par ordonnance du 19 juillet 2018, la Cour a suspendu le traitement de l'affaire *sine die*.

Par ordonnance du 21 avril 2021, la Cour, après avoir entendu les juges-rapporteurs D. Pieters, en remplacement du président émérite A. Alen, et T. Giet, en remplacement du juge J.-P. Moerman, légitimement empêché, a décidé :

- de rouvrir les débats,

- d'inviter les parties à exposer, dans un mémoire complémentaire à introduire le 31 mai 2021 au plus tard et à communiquer aux autres parties dans le même délai, leur point de vue sur l'incidence de l'arrêt de la Cour de justice de l'Union européenne du 6 octobre 2020 dans les affaires n^{os} C-511/18, C-512/18 et C-520/18 et de l'arrêt de la Cour constitutionnelle n° 57/2021 du 22 avril 2021 sur le présent recours en annulation,

- qu'aucune audience ne serait tenue, à moins qu'une partie n'ait demandé, dans le délai de sept jours suivant la réception de la notification de la présente ordonnance, à être entendue,

- qu'en cas d'une telle demande, l'affaire serait prise à l'audience du 16 juin 2021, à l'heure ultérieurement fixée par le président, et

- qu'en l'absence d'une telle demande, les débats seraient clos le 16 juin 2021 et l'affaire mise en délibéré.

Des mémoires complémentaires ont été introduits par :

- les parties requérantes;

- le Conseil des ministres, assisté et représenté par Me S. Depré, Me E. de Lophem et Me G. Ryelandt.

À la suite de la demande du Conseil des ministres à être entendu, le président, par ordonnance du 5 mai 2021, a fixé l'heure de l'audience du 16 juin 2021 à 14.00 heures.

À l'audience publique du 16 juin 2021 :

- ont comparu :

. Me D. Pattyn, pour les parties requérantes, et Patrick Van Assche, en personne;

. Me E. de Lophem et Me G. Ryelandt, qui comparaissaient également *loco* Me S. Depré, pour le Conseil des ministres;

- les juges-rapporteurs D. Pieters et J.-P. Moerman ont fait rapport;

- les parties précitées ont été entendues;

- l'affaire a été mise en délibéré.

Les dispositions de la loi spéciale du 6 janvier 1989 sur la Cour constitutionnelle relatives à la procédure et à l'emploi des langues ont été appliquées.

II. *En droit*

- A -

Quant à la recevabilité du recours

A.1. Les parties requérantes exposent qu'elles sont confrontées à une obligation d'identification en leur qualité d'utilisateurs finaux de services de téléphonie au moyen de cartes prépayées. Le traitement, la conservation et la communication des données à caractère personnel mentionnées dans la loi attaquée entraînent selon elles une ingérence excessive dans leur vie privée, étant donné que l'identification obligatoire des utilisateurs finaux de services de téléphonie permet d'établir un lien entre les parties requérantes et leurs données de trafic et de localisation.

Elles font valoir en outre qu'en leur qualité de conseillers communaux de la commune de Brecht, elles bénéficient d'un droit renforcé à la liberté d'expression, qui comprend le droit de recevoir et de transmettre des informations, notamment sur la base de télécommunications anonymes.

A.2.1. Le Conseil des ministres observe que les différentes critiques que les parties requérantes formulent dans le cadre du recours en annulation présentement examiné portent en réalité sur la loi du 29 mai 2016 « relative à la collecte et à la conservation des données dans le secteur des communications électroniques ». Les mêmes parties requérantes ont introduit un recours en annulation contre cette loi, qui a été inscrit sous le numéro 6601 du rôle de la Cour. Pour autant que les critiques des parties requérantes portent en réalité sur cette loi, et non sur la loi attaquée, le recours en annulation n'est pas recevable *ratione temporis*.

A.2.2. Les parties requérantes soulignent qu'elles déduisent en partie l'inconstitutionnalité de la loi attaquée des conséquences qui en découlent lorsqu'elle est lue en combinaison avec la loi du 29 mai 2016. Pour apprécier la constitutionnalité de la loi attaquée, la Cour doit donc tenir compte de la loi du 29 mai 2016, même en tant que le recours en annulation est dirigé contre la loi attaquée, lue en combinaison avec la loi du 29 mai 2016.

Quant au premier moyen

A.3.1. Dans leur premier moyen, les parties requérantes font valoir que l'article 2 de la loi attaquée n'est pas compatible avec les articles 10, 11 et 22 de la Constitution, lus en combinaison avec l'article 8 de la Convention européenne des droits de l'homme, avec les articles 7, 8 et 52 de la Charte des droits fondamentaux de l'Union européenne, et avec les articles 2, point a), et 6 de la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 « relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données ».

Dans leur requête, elles allèguent que l'habilitation conférée au Roi pour fixer les mesures techniques et administratives imposées aux canaux de vente des services de communications électroniques et aux entreprises fournissant un service d'identification, n'a pas été définie de manière suffisamment précise, qu'elle n'est pas limitée à la mise en œuvre de mesures dont les éléments essentiels ont été fixés au préalable par le législateur, et qu'elle ne garantit pas que les données et documents d'identification collectés sont pertinents et proportionnels à la lumière des objectifs pour lesquels ils sont traités.

A.3.2. Les parties requérantes exposent que l'article 127 de la loi du 13 juin 2005 « relative aux communications électroniques », modifié par la disposition attaquée, autorise le Roi à fixer les mesures techniques et administratives imposées aux opérateurs offrant au public des services de télécommunications afin d'identifier l'utilisateur final. Cette disposition vise autant les magasins des opérateurs eux-mêmes que tous les autres canaux de vente, tels que les supermarchés ou les *night shops*, même si ces derniers canaux ne conservent pas de données et documents d'identification. La disposition attaquée s'applique également aux cartes prépayées d'opérateurs étrangers qui sont vendues en Belgique. À partir de l'entrée en vigueur de l'arrêté d'exécution, les nouvelles cartes prépayées ne pourront plus être activées sans identification de l'utilisateur final. Les anciennes cartes prépayées

doivent être identifiées dans un délai de six mois à partir de l'entrée en vigueur de l'arrêté d'exécution, sous peine d'être déconnectées par l'opérateur.

A.3.3. Les parties requérantes soulignent dans leur requête la corrélation entre la disposition attaquée et la loi du 29 mai 2016 « relative à la collecte et à la conservation des données dans le secteur des communications électroniques ». Cette loi impose aux fournisseurs de services de télécommunications une obligation de conservation généralisée et indifférenciée. Ils sont tenus de conserver les données d'identification, les données de connexion et de localisation et les données de communications de leurs clients. Ces données ne portent pas sur le contenu, mais sur l'origine et la destination de la communication. La loi du 29 mai 2016 règle l'accès aux données conservées et crée également une cellule de coordination commune des fournisseurs et des opérateurs, qui est chargée de fournir cet accès. Les informations collectées par les fournisseurs de services de télécommunications sur la base de la disposition attaquée doivent également être conservées dans le cadre de la loi du 29 mai 2016.

A.3.4. Selon les parties requérantes, le traitement des données à caractère personnel qui consiste à collecter les données d'identification visées par la disposition attaquée limite le droit au respect de la vie privée. Il en va de même pour la conservation de ces données et pour l'accès à celle-ci en vertu de la loi du 29 mai 2016.

Selon les parties requérantes, l'article 22, alinéa 1er, de la Constitution exige qu'une telle limitation trouve son fondement dans une loi formelle. Une délégation au Roi ne serait possible que si l'habilitation a été définie de manière suffisamment précise et se rapporte à l'exécution de mesures dont les éléments essentiels ont été fixés au préalable par le législateur. La Cour de justice a elle aussi jugé dans son arrêt du 8 avril 2014 (C-293/12 et C-594/12) que le droit au respect de la vie privée ne peut être limité que sur la base d'une loi formelle.

A.3.5.1. Selon les parties requérantes, la disposition attaquée accorde une délégation excessive au Roi, parce qu'elle L'autorise à fixer les mesures techniques et administratives imposées aux fournisseurs et opérateurs, aux canaux de vente de services de communications électroniques et aux entreprises fournissant un service d'identification, entre autres pour identifier l'utilisateur final. De plus, la disposition attaquée introduit une présomption en vertu de laquelle la personne identifiée est réputée, jusqu'à preuve du contraire, utiliser elle-même le service de communications électroniques.

La Commission de la protection de la vie privée (ci-après : la CPVP) a critiqué le projet de loi qui a conduit à la loi attaquée, étant donné que le législateur aurait négligé de régler dans la loi certains éléments essentiels de la réglementation attaquée, comme la désignation du responsable du traitement, la liste des personnes ayant accès aux données et la fixation du délai de conservation (avis n° 54/2015 du 16 décembre 2015). Cette critique a été réitérée par la section de législation du Conseil d'État dans son avis sur la loi attaquée. Selon les parties requérantes, le législateur n'a pas suffisamment répondu à ces critiques dès lors qu'il n'a pas désigné les données d'identification à collecter, qu'il n'a pas précisé les documents d'identification dont la force probante peut être admise et qu'il n'a pas fixé de critères pour encadrer la délégation au Roi par rapport à la différenciation entre les anciennes et les nouvelles cartes prépayées.

A.3.5.2. Selon les parties requérantes, le type d'informations qui peuvent être conservées constitue un élément essentiel que le législateur doit régler et qu'il ne peut déléguer au Roi. En vertu de la disposition attaquée, le Roi dispose d'un pouvoir discrétionnaire trop important pour règlementer le type d'informations qui sont collectées et conservées, étant donné que la disposition attaquée ne précise pas ce qu'il faut entendre par « données et documents d'identification ». Ainsi, l'on n'aperçoit pas clairement s'il peut s'agir de données se rapportant à l'identité physique, physiologique, psychique, économique, culturelle ou sociale de l'utilisateur final. Le manque de délimitation permet au Roi de prendre toute donnée à caractère personnel en considération dans le cadre de la disposition attaquée.

A.3.5.3. Les catégories de personnes à propos desquelles des informations peuvent être collectées constituent elles aussi un élément essentiel qui ne saurait être délégué au Roi. La disposition attaquée mentionne seulement « l'utilisateur final ». L'article 2, 13°, de la loi du 13 juin 2005 définit un utilisateur final comme celui qui ne fournit pas de réseau public de communications électroniques ou de services de communications électroniques accessibles au public. L'article 2, 12°, de la même loi définit un utilisateur comme la personne physique ou morale qui utilise ou demande un service de communications électroniques accessible au public. Le législateur accorde

donc au Roi un pouvoir discrétionnaire qui Lui permet d'imposer une obligation d'identification à toutes les personnes physiques ou morales qui font usage d'un réseau de communications électroniques, sans en fournir un elles-mêmes.

A.3.5.4. Selon les parties requérantes, les circonstances dans lesquelles le traitement de données peut être effectué, les personnes qui ont le droit de consulter les informations enregistrées et le délai maximum de conservation des données constituent également des éléments essentiels. À cet égard, la disposition attaquée se borne à indiquer que les services de renseignement et de sécurité peuvent requérir le concours d'une banque ou d'une institution financière pour procéder à l'identification de l'utilisateur final, ainsi qu'au constat de ce que la conservation des données collectées s'effectue en vertu de l'article 126, § 3, alinéa 1er, de la loi du 1er septembre 2016. En fait, la disposition attaquée permet au Roi d'étendre sensiblement le champ d'application et le contenu de la loi du 29 mai 2016.

A.3.5.5. Enfin, les sanctions en cas de non-respect de l'obligation d'identification constituent également un élément essentiel. Cependant, la disposition attaquée interdit aux fournisseurs de continuer à offrir des services de communications électroniques s'ils ne se conforment pas aux mesures techniques et administratives définies par le Roi. Ils doivent en outre fermer le service de communications électroniques des utilisateurs finaux qui ne respectent pas les obligations établies par le Roi. Ces sanctions représentent une atteinte grave au droit à la liberté d'expression des utilisateurs finaux, de sorte que l'on ne peut laisser au Roi la compétence de définir le contenu des obligations sanctionnées.

A.3.6. De façon plus générale, la disposition attaquée ne garantit pas, selon les parties requérantes, que le règlement élaboré par le Roi présente un caractère pertinent et non excessif au regard des finalités pour lesquelles les données à caractère personnel énumérées par le Roi sont traitées.

A.4.1. Le Conseil des ministres souligne que les dispositions constitutionnelles qui réservent une compétence au législateur n'instaurent aucune interdiction absolue de procéder à une délégation. Il est permis au législateur de déléguer au Roi une compétence délimitée avec précision, pour autant qu'il règle lui-même les éléments essentiels de cette matière.

Le Conseil des ministres relève à cet égard que la disposition attaquée ne contient quasiment pas de délégations au Roi. Seul l'article 127, § 3, alinéa 2, de la loi du 1er septembre 2016 délègue au Roi la compétence de définir la notion « d'utilisateur final non identifié ». Les parties requérantes n'ont pas critiqué cette délégation. Les autres délégations contestées par les parties requérantes figuraient déjà dans la loi du 13 juin 2005, avant qu'elle soit modifiée par la loi du 1er septembre 2016. Dans cette mesure, le premier moyen n'est dès lors pas recevable.

Les avis de la CPVP et de la section de législation du Conseil d'État qui sont cités par les parties requérantes ne sont d'ailleurs pas pertinents, puisque le législateur a mis en œuvre ces avis en incluant dans la disposition attaquée les éléments essentiels requis.

Le Conseil des ministres fait en outre valoir que ce n'est pas la loi du 1er septembre 2016 qui permet l'identification des utilisateurs de cartes prépayées. Ce principe avait déjà été consacré par l'article 127, § 3, alinéa 1er, de la loi du 13 juin 2005, et n'a pas été modifié par la disposition attaquée.

A.4.2. Par rapport au type d'informations pouvant être conservées, le Conseil des ministres soutient que le législateur ne délègue nullement au Roi le pouvoir de déterminer ce qu'il faut entendre par « données ou documents d'identification ». Ces notions ont été insérées par l'article 127, § 1er, alinéa 8, de la loi du 13 juin 2005, sans que le Roi soit autorisé à les définir plus amplement. La section de législation du Conseil d'État n'a d'ailleurs formulé aucune observation à cet égard.

Le seul élément essentiel qu'il fallait régler dans la loi est le principe même de l'identification. La méthode, les données et les documents concernés par cette identification ne constituent pas des éléments essentiels de la limitation contestée qui est apportée au droit au respect de la vie privée et familiale, mais n'en sont que des modalités.

S'il devait s'avérer que le Roi a quand même prévu des données et documents d'identification non compatibles avec les exigences du respect de la vie privée, il est possible de contester l'arrêté royal en question devant la section du contentieux administratif du Conseil d'État.

A.4.3. En ce qui concerne les catégories de personnes à propos desquelles des informations peuvent être recueillies, le Conseil des ministres soutient qu'elles ne font pas l'objet de la disposition attaquée, mais qu'elles étaient déjà réglées par l'article 127, § 1er, 2°, de la loi du 13 juin 2005, avant sa modification par la loi attaquée.

De plus, l'intention formelle du législateur est d'imposer une obligation d'identification à tous les utilisateurs finaux au sens de l'article 2, 13°, de la loi du 13 juin 2005, de sorte qu'il n'est pas nécessaire de donner au Roi une délégation sur ce point.

A.4.4. De même, les circonstances dans lesquelles le traitement de données peut être effectué, les personnes qui ont le droit de consulter les informations conservées et le délai de conservation maximum des données étaient déjà prévus par l'article 127 de la loi du 13 juin 2005, avant sa modification par la loi attaquée. Cette disposition fait d'ailleurs référence à l'article 126 de la même loi, qui précise les autorités qui ont accès aux données conservées et le délai dans lequel cet accès doit avoir lieu.

A.4.5. Les sanctions en cas de non-respect de l'obligation d'identification ont également été définies intégralement par l'article 127, §§ 4 et 5, de la loi du 13 juin 2005, si bien qu'il ne subsiste aucune marge pour conférer une délégation au Roi.

A.5.1. Les parties requérantes font remarquer que lorsque le législateur légifère à nouveau dans une matière donnée, et qu'il étend à cet égard une délégation au Roi qui existait déjà, la Cour est compétente pour connaître d'un recours introduit contre cette extension. La disposition attaquée rend l'article 127 de la loi du 13 juin 2005 beaucoup plus strict puisqu'elle a transformé l'identification facultative de l'utilisateur final en une identification obligatoire. Elle réalise cette transformation sur la base de plusieurs délégations au Roi. De plus, la disposition attaquée interdit la vente de nouvelles cartes prépayées et impose la mise hors service des anciennes cartes prépayées dont le propriétaire ne s'identifie pas dans le délai fixé par le Roi.

D'ailleurs, les articles 37 et 108 de la Constitution n'imposent au Roi aucune habilitation expresse pour établir les règlements et prendre les arrêtés nécessaires à l'exécution des lois. La disposition attaquée confère donc au Roi une habilitation implicite pour réglementer une matière réservée au législateur par l'article 22, alinéa 1er, de la Constitution.

Rien n'empêche la disposition attaquée d'habiliter formellement le Roi à définir les mesures techniques et administratives imposées aux canaux de vente de services de communications électroniques et aux entreprises qui fournissent un service d'identification, notamment en ce qui concerne l'identification de l'utilisateur final. Ce qui précède n'interdit pas non plus que les données et documents d'identification collectés soient conservés conformément à l'article 126, § 3, alinéa 1er, de la loi du 13 juin 2005, ni que l'article 127, §§ 4 et 5, de la même loi définisse les sanctions imposées aux opérateurs et aux fournisseurs de services de communications électroniques qui ne satisfont pas aux mesures techniques et administratives imposées par le Roi.

Enfin, les parties requérantes soulignent que le préambule de l'arrêté royal du 27 novembre 2016 « relatif à l'identification de l'utilisateur final de services de communications électroniques publics mobiles fournis sur la base d'une carte prépayée » précise que cet arrêté royal trouve son fondement dans l'article 127, § 1er, de la loi du 13 juin 2005, tel qu'il a été modifié en dernier lieu par la loi du 1er septembre 2016.

A.5.2.1. En outre, par rapport au type d'informations qui peuvent être conservées, la disposition attaquée ne définit pas des notions essentielles telles que les « données ou documents d'identification », alors que la CPVP et la section de législation du Conseil d'État avaient toutes deux insisté sur ce point. Il apparaît du reste de l'arrêt *Rotaru c. Roumanie* du 4 mai 2000 de la Cour européenne des droits de l'homme que le type d'informations récoltées constitue effectivement un élément essentiel que doit régler le législateur.

A.5.2.2. En ce qui concerne les catégories de personnes à propos desquelles des informations peuvent être recueillies, les parties requérantes répètent que l'identification des utilisateurs finaux de cartes prépayées était auparavant facultative et que la disposition attaquée a rendu cette identification obligatoire. Elle étend par ailleurs l'habilitation conférée au Roi pour définir les mesures techniques et administratives, en vue d'identifier l'utilisateur final, aux canaux de vente de services de communications électroniques et aux entreprises qui fournissent un service d'identification.

A.5.2.3. En ce qui concerne les circonstances dans lesquelles le traitement de données peut être effectué, les personnes qui ont le droit de consulter les informations conservées et le délai de conservation maximum des

données, les parties requérantes estiment que l'argumentation du Conseil des ministres est hors de propos. Le Roi dispose d'un pouvoir d'appréciation trop large pour déterminer les données ou documents d'identification qui doivent être collectés et les catégories d'utilisateurs finaux qui sont soumises à l'obligation d'identification.

A.5.2.4. Quant aux conséquences du non-respect de l'obligation d'identification, les parties requérantes soulignent que le Roi peut décider que même la moindre infraction peut donner lieu à la non-fourniture ou à la déconnection des services de communications électroniques. Un tel système de sanctions est disproportionné par rapport à l'objectif poursuivi.

A.6. Le Conseil des ministres constate que les parties requérantes déduisent, non pas de la disposition attaquée, mais de l'article 126 de la loi du 13 juin 2005, non modifié par la disposition attaquée, et du rapport au Roi annexé à l'arrêté royal du 27 novembre 2016, que le législateur a accordé une délégation au Roi. De tels éléments ne peuvent toutefois pas être pris en considération pour juger de la constitutionnalité de la disposition attaquée.

A.7. Les parties requérantes allèguent dans leur mémoire complémentaire que l'annulation de l'article 126 de la loi du 13 juin 2005 par l'arrêt de la Cour n° 57/2021 du 22 avril 2021 rend encore plus incertaine la base légale de la restriction apportée à la vie privée et qui est dénoncée. La disposition attaquée habilite en effet le Roi à régler le traitement des données contesté en vue d'une obligation de conservation que la Cour a annulée. À la suite de cette annulation, la conservation des données à caractère personnel visée dans la disposition attaquée n'est plus soumise à aucune condition. Aucune disposition législative ne régit actuellement les données à conserver, les personnes concernées par le traitement des données ni les conditions et finalités du traitement. La base légale du traitement initial des données visé dans la disposition attaquée est donc atteinte elle aussi.

A.8. Le Conseil des ministres observe dans son mémoire complémentaire qu'une nouvelle réglementation sur la conservation des données, qui satisfait aux exigences mentionnées dans l'arrêt de la Cour n° 57/2021, est actuellement en préparation. La base légale pour le traitement des données sera donc restaurée rapidement.

Quant au deuxième moyen

A.9. Dans leur deuxième moyen, les parties requérantes font valoir que les articles 2 et 3 de la loi attaquée ne sont pas compatibles avec les articles 10, 11, 19, 22 et 25 de la Constitution, lus en combinaison avec les articles 8 et 10 de la Convention européenne des droits de l'homme, avec les articles 7, 8 et 52 de la Charte des droits fondamentaux de l'Union européenne, avec les articles 56 et 57 du Traité sur le fonctionnement de l'Union européenne, avec les articles 2, point a), et 6 de la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 « relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données » et avec les articles 1er, 2, 3, 5, 6, 9 et 15 de la directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 « concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques) ». Le moyen se subdivise en trois branches.

La première branche du deuxième moyen

A.10. Dans la première branche du deuxième moyen, les parties requérantes reprochent à la loi attaquée d'instaurer une obligation d'identification généralisée et indifférenciée pour tous les utilisateurs finaux de tous les services de communications électroniques, qui constitue une ingérence injustifiée dans le droit à la protection de la vie privée.

A.11.1. Les parties requérantes exposent que l'article 127 de la loi du 13 juin 2005, modifié par l'article 2 de la loi attaquée, vise à supprimer l'anonymat des cartes prépayées des opérateurs mobiles. La vente de nouvelles cartes prépayées anonymes est interdite, tandis que l'identification des utilisateurs finaux d'anciennes cartes prépayées est obligatoire. Cette obligation doit être combinée avec la loi du 29 mai 2016, qui impose une obligation de conservation généralisée et indifférenciée aux fournisseurs de services d'internet et de téléphonie au public en

vue d'identifier et de localiser l'utilisateur final ou l'abonné. En effet, conformément aux dispositions attaquées, les données qui sont recueillies doivent être conservées et communiquées en suivant les procédures établies par la loi du 29 mai 2016.

A.11.2.1. Selon les parties requérantes, la directive 2002/58/CE s'applique au traitement des données à caractère personnel dans le cadre de la fourniture de services de communications électroniques accessibles au public sur les réseaux publics de communications dans l'Union européenne. Les données d'identification collectées en vertu de la loi attaquée constituent des données à caractère personnel au sens de cette directive. Il ressort de la jurisprudence de la Cour de justice de l'Union européenne qu'il en va de même pour le traitement et la conservation de données de communications dans le cadre de la sauvegarde de la sécurité nationale et de la défense, et pour la détection et la poursuite d'infractions pénales. La loi attaquée relève donc du champ d'application du droit de l'Union européenne.

A.11.2.2. Les dispositions attaquées, ainsi que la conservation des données d'identification collectées en vertu de la loi du 29 mai 2016, constituent en outre une limitation du droit au respect de la vie privée et familiale, comme en atteste d'ailleurs l'arrêt de la Cour n° 108/2016 du 14 juillet 2016.

A.11.2.3. Selon la jurisprudence de la Cour de justice de l'Union européenne, une telle limitation ne peut se justifier que s'il y a un contrôle juridictionnel strict du respect du principe de proportionnalité. Ce contrôle de proportionnalité exige de vérifier que le but poursuivi peut être réalisé par la conservation des données, que les exceptions à la protection des données à caractère personnel restent dans les limites du strict nécessaire et que la collecte de données à caractère personnel s'effectue dans le cadre de règles claires et précises régissant la portée et l'application de la mesure en question. Ces règles doivent prévoir des critères objectifs qui limitent l'accès des autorités nationales compétentes aux données à caractère personnel. Leur application doit également être soumise à un contrôle préalable d'une juridiction ou d'une autorité administrative indépendante. De plus, le délai de conservation de ces données doit être adapté à l'objectif pour lequel les données sont conservées. Enfin, les données collectées doivent être protégées contre un accès illicite.

A.11.3.1. Il est précisé dans les travaux préparatoires des dispositions attaquées que la suppression de l'anonymat des cartes prépayées répond à une demande des autorités judiciaires, des services de renseignement et de sécurité, et des services d'urgence. Étant donné que les cartes prépayées sont très répandues dans les milieux criminels, l'identification de l'utilisateur final est cruciale dans la lutte contre le terrorisme et pour la détection et la poursuite d'infractions pénales graves. Toute autre technique pour identifier l'utilisateur final engendrerait d'ailleurs une plus grande ingérence dans la vie privée et familiale que le simple accès à des données et documents collectés au préalable. D'ailleurs, les titulaires d'un abonnement de téléphonie ne sont pas anonymes, et ce sont uniquement les titulaires de cartes de téléphone prépayées qui ne peuvent être identifiés jusqu'à présent. L'anonymat des cartes prépayées avait d'ailleurs toujours été conçu comme une mesure temporaire pour soutenir la pénétration du GSM sur le marché belge.

A.11.3.2. Les parties requérantes estiment que seule la lutte contre la criminalité grave et le terrorisme peut justifier l'obligation d'identification contestée. En revanche, les autres objectifs cités dans les travaux préparatoires ne peuvent entrer en ligne de compte dans le cadre de la limitation d'un droit fondamental tel que le respect de la vie privée et familiale. Selon les parties requérantes, il ressort également de la jurisprudence de la Cour de justice concernant l'article 15, paragraphe 1, de la directive 2002/58/CE que la possibilité offerte par cette disposition de traiter des données à caractère personnel dans le cadre de la sécurité nationale peut seulement être utilisée pour les objectifs que cette disposition énumère limitativement. Il ressortirait également de cette jurisprudence que cet objectif ne peut pas être invoqué pour faire du stockage de données à caractère personnel la règle. Bien que la lutte contre la criminalité grave et le terrorisme dépende en grande partie du recours à des technologies modernes, un tel objectif ne peut en effet pas conduire à une réglementation nationale prévoyant une conservation généralisée et indifférenciée de toutes les données de trafic et de localisation.

A.11.4.1. L'obligation d'identification contestée n'est pas proportionnelle à l'objectif de lutte contre la criminalité grave et le terrorisme. Premièrement, elle est inadéquate pour atteindre cet objectif, étant donné qu'elle n'interdit pas de céder à un tiers une carte prépayée. Par ailleurs, un téléphone portable qui utilise une carte prépayée peut également être volé. Dans de tels cas, les dispositions attaquées conduisent plutôt à l'identification d'une personne qui n'a rien à voir avec le délit qui est instruit, tandis que l'auteur n'est pas identifié. Deuxièmement, les dispositions attaquées n'empêchent pas l'utilisation en Belgique de cartes prépayées anonymes achetées à l'étranger, sur la base du *roaming* international. Troisièmement, il existe plusieurs formes de

communications électroniques qui ne sont pas visées par les dispositions attaquées et qui peuvent également servir dans le cadre d'activités criminelles et terroristes.

A.11.4.2. Les parties requérantes regrettent par ailleurs l'absence de règles claires et précises sur la portée et l'application de la loi attaquée. Celle-ci ne désigne effectivement pas les données à caractère personnel pouvant être collectées, les catégories de personnes à identifier, les modalités et la durée de conservation des données et les titulaires d'un accès à celles-ci.

Il est dès lors également impossible de déterminer si les données collectées sont strictement nécessaires par rapport à l'objectif d'une lutte efficace contre le terrorisme et la criminalité grave.

A.11.4.3. De même, l'accès aux données collectées et la protection et la sécurisation de ces données ne sont pas suffisamment réglés. La seule chose claire, c'est que ces données sont conservées en vertu de l'article 126 de la loi du 13 juin 2005, tel qu'il a été modifié pour la dernière fois par la loi du 29 mai 2016. Il ressort du recours en annulation que les parties requérantes ont introduit contre cette loi, que la Cour a inscrit sous le numéro 6601 du rôle, que cette disposition n'est nullement suffisante puisqu'elle ne règle pas la confidentialité des données.

A.12.1. Le Conseil des ministres estime que la référence aux directives 95/46/CE et 2002/58/CE repose sur une analyse inexacte de la portée de la loi attaquée. En effet, cette loi ne porte nullement sur les données de communications, de localisation ou de trafic au sens de ces directives, mais seulement sur l'identification du titulaire d'une carte prépayée au moment où il achète ladite carte. La loi ne traite pas d'autres données à caractère personnel que l'identité de l'acheteur.

A.12.2. Les parties requérantes ne démontrent nullement que le droit à la protection de la vie privée impliquerait également un droit à l'anonymat. C'est dans ce sens qu'il y a lieu d'établir une distinction entre le contenu de la loi attaquée et celui de la loi du 29 mai 2016, qui règle effectivement un traitement de données à caractère personnel. Les dispositions attaquées ne règlent pas les modalités d'utilisation d'une carte prépayée, mais seulement l'identification de l'utilisateur final.

A.12.3. Cette identification est nécessaire dans le cadre d'une lutte efficace contre la criminalité grave et le terrorisme. De plus en plus de pays européens adoptent une réglementation similaire. S'il devait s'avérer que cette mesure n'est pas parfaite et qu'elle peut être contournée par des criminels habiles, il conviendrait de la renforcer; il ne peut toutefois s'en déduire que les dispositions attaquées ne seraient pas nécessaires sous leur forme actuelle. Bon nombre de lacunes que les parties requérantes soulèvent sont d'ailleurs expressément réglées par d'autres dispositions légales et réglementaires. Ainsi, l'arrêté royal du 27 novembre 2016 règle le cas de la vente ou du vol de cartes prépayées. Le risque de *roaming* international est quant à lui réglé par l'article 6*ter* du règlement (UE) 2015/2120 du Parlement européen et du Conseil du 25 novembre 2015 « établissant des mesures relatives à l'accès à un internet ouvert et modifiant la directive 2002/22/CE concernant le service universel et les droits des utilisateurs au regard des réseaux et services de communications électroniques et le règlement (UE) n° 531/2012 concernant l'itinérance sur les réseaux publics de communications mobiles à l'intérieur de l'Union ».

Les parties requérantes n'exposent d'ailleurs pas pourquoi il faudrait maintenir en l'espèce une différence de traitement entre les cartes prépayées et les abonnements.

A.13.1. Les parties requérantes répondent qu'en vertu de l'article 2, point a), de la directive 95/46/CE, toute information relative à une personne physique identifiée ou identifiable est une donnée à caractère personnel. Les données qui sont requises en vertu des dispositions attaquées pour identifier l'utilisateur final constituent donc des données à caractère personnel. Au demeurant, il ressort de la jurisprudence de la Cour de justice de l'Union européenne que les activités des fournisseurs de services de communications électroniques relèvent du champ d'application de la directive 2002/58/CE.

Le fait que la loi attaquée porte uniquement sur des données d'identification n'empêche pas que ces données doivent être traitées en vertu de la loi du 29 mai 2016. La loi attaquée a pour conséquence que les simples données d'identification doivent également être conservées par les fournisseurs et les opérateurs, et qu'elles sont traitées selon des modalités approuvées par les autorités et qui permettent de les utiliser.

A.13.2. Selon les parties requérantes, il ressort d'une étude scientifique et d'articles de presse que l'obligation d'identification n'est pas nécessaire et n'est pas efficace dans la lutte contre la criminalité grave et le

terrorisme. Par définition, une mesure qui ne peut pas être efficace n'est pas non plus proportionnée à l'objectif poursuivi.

La volonté de supprimer la prétendue différence de traitement entre les utilisateurs finaux de cartes prépayées et les titulaires d'un abonnement de téléphonie ne peut justifier la mesure attaquée, étant donné que celle-ci est sans rapport avec la sécurité nationale, le bien-être économique du pays, la lutte contre la criminalité grave ou la santé publique.

A.13.3. L'arrêté royal du 27 novembre 2016 mentionné par le Conseil des ministres n'empêche pas que l'utilisateur effectif d'une carte prépayée ne puisse pas être identifié sur la base des données d'identification de l'acheteur. Les parties requérantes ajoutent que des personnes morales peuvent contourner facilement l'obligation d'identification.

Le règlement (UE) 2015/2120, mentionné par le Conseil des ministres, ne fait pas non plus obstacle à ce qu'une carte prépayée achetée à l'étranger permette, grâce au *roaming* international, de contourner les dispositions attaquées. D'ailleurs, ce règlement ne sanctionne pas l'utilisation abusive du *roaming* international par le blocage de cette carte, mais seulement par le paiement d'un supplément. Un tel supplément n'intimidera pas le crime organisé ou les groupements terroristes.

A.13.4. Les dispositions attaquées ont donc surtout des conséquences négatives pour des particuliers, alors que les personnes morales, les organisations criminelles et les organisations terroristes peuvent facilement en contourner le fonctionnement. Les dispositions attaquées risquent donc de toucher des personnes vulnérables incapables de s'identifier simplement, notamment les étrangers.

A.14. Le Conseil des ministres soutient que les cartes des personnes qui éprouvent des difficultés à s'identifier ne seront pas désactivées immédiatement. Dans un premier temps, on essayera à nouveau de les identifier. Les documents dont disposent les étrangers enregistrés satisfont d'ailleurs aux standards d'identification.

A.15. Les parties requérantes soulignent dans leur mémoire complémentaire que, par son arrêt du 6 octobre 2020, en cause *La Quadrature du Net e.a.* (C-511/18) , la Cour de justice a jugé qu'une conservation généralisée et indifférenciée des données d'identification ne peut être prévue que sur la base de « règles claires et précises [qui assurent] que la conservation des données en cause est subordonnée au respect des conditions matérielles et procédurales y afférentes et que les personnes concernées disposent de garanties effectives contre les risques d'abus ». Ce cadre juridique clair et précis n'existe plus après l'annulation, par l'arrêt n° 57/2021, de la réglementation concernant la conservation des données. Dès lors que les dispositions relatives à la Cellule de coordination ont elles aussi été annulées, la confidentialité des données d'identité conservées n'est pas garantie.

A.16.1. Le Conseil des ministres attire l'attention dans son mémoire complémentaire sur la distinction entre la réglementation annulée concernant la conservation des données et la disposition actuellement attaquée. La disposition attaquée ne porte pas sur les données de trafic et de localisation. Les données d'identification du titulaire d'une carte prépayée ne sont pas traitées comme des « données de trafic » au sens de l'article 2, 6°, de la loi du 13 juin 2005, dès lors qu'il ne reçoit pas de facture. Seules les données d'identification de l'utilisateur final d'une carte prépayée sont donc traitées. Ses données ne sont en aucun cas traitées pour la transmission d'une communication sur un réseau de communications électroniques. La loi attaquée ne porte pas sur l'accès aux données stockées : celui-ci est réglé dans la législation organique des organes qui peuvent avoir accès à ces données. Cette législation n'est pas attaquée présentement.

A.16.2. Le Conseil des ministres attire aussi l'attention dans son mémoire complémentaire sur le fait que, par l'arrêt du 6 octobre 2020 en cause *La Quadrature du Net e.a.* (C-511/18), la Cour de justice a jugé que l'article 15, paragraphe 1, de la directive 2002/58/CE ne s'oppose pas à une conservation généralisée et indifférenciée de simples données d'identification. En effet, l'identité civile ne permet pas de connaître la date, l'heure, la durée et les destinataires des communications effectuées, non plus que les endroits où ces communications ont eu lieu ou la fréquence de celles-ci avec certaines personnes pendant une période donnée. Une telle ingérence dans la vie privée n'a pas été qualifiée d'ingérence grave par la Cour de justice.

La deuxième branche du deuxième moyen

A.17. Dans la deuxième branche du deuxième moyen, les parties requérantes reprochent à l'obligation d'identification instaurée par les dispositions attaquées de freiner l'exercice de la libre circulation des services, alors que cette limitation n'est pas appropriée dans le cadre de la lutte contre la criminalité grave et le terrorisme et va au-delà de ce qui est nécessaire pour atteindre cet objectif.

A.18.1.1. Selon les parties requérantes, les articles 56 et 57 du Traité sur le fonctionnement de l'Union européenne interdisent que soit imposée à un prestataire de services qui est établi dans un autre État membre et qui y fournit légitimement des services, toute mesure nationale l'empêchant de proposer des services similaires sur le territoire national. De telles restrictions ne sont admissibles que si elles poursuivent un but d'intérêt général, si elles sont appropriées pour atteindre le but visé et ne vont pas au-delà de ce qui est nécessaire pour réaliser l'objectif fixé. Au demeurant, une réglementation légale nationale qui limite la libre prestation de services pour des motifs impérieux d'intérêt général n'est appropriée pour réaliser l'objectif fixé que si cette réalisation est poursuivie d'une manière cohérente et systématique.

A.18.1.2. Les parties requérantes soutiennent que la loi du 13 juin 2005 s'applique à quiconque fournit habituellement contre rémunération un service qui consiste entièrement ou principalement à transmettre des signaux sur des réseaux de communications électroniques. De telles prestations relèvent du champ d'application des articles 56 et 57 du Traité sur le fonctionnement de l'Union européenne. Les dispositions attaquées s'appliquent d'ailleurs sans distinction tant aux opérateurs nationaux qu'aux opérateurs étrangers qui proposent en Belgique des cartes prépayées. Il suffit que cette carte soit reliée à un numéro de téléphone belge ou à une IMSI (*International Mobile Subscriber Identity*) belge, ou que la carte prépayée soit vendue en Belgique.

A.18.2. L'obligation d'identification implique que tous les prestataires de services qui relèvent du champ d'application des dispositions attaquées doivent procéder à l'identification des utilisateurs finaux et doivent respecter les mesures techniques et administratives fixées par le Roi. Il leur est interdit de proposer des services de communications électroniques qui ne répondent pas à ces conditions. Ils doivent en outre désactiver les anciennes cartes prépayées des utilisateurs finaux qui refusent de s'identifier et doivent refuser d'activer les nouvelles cartes prépayées si l'acheteur refuse de s'identifier. Ces mesures entravent la libre circulation des services ou à tout le moins la rendent moins accessible.

A.18.3. Les parties requérantes déduisent de l'exposé de la première branche du deuxième moyen que les dispositions attaquées ne sont pas appropriées au regard de la lutte contre la criminalité grave et le terrorisme. Il en va d'autant plus ainsi que l'obligation d'identification qui est contestée ne fait pas l'objet d'une législation harmonisée au niveau de l'Union européenne. Sur la base du *roaming* international, des utilisateurs belges peuvent donc acheter une carte prépayée à l'étranger et rester ainsi anonymes, mais il devient néanmoins plus difficile, pour des opérateurs étrangers, de proposer leurs services en Belgique.

A.19.1. Selon le Conseil des ministres, les dispositions attaquées ne limitent aucunement la libre circulation des services. Toute norme législative qui impose une obligation aux entreprises n'a pas un effet restrictif sur la libre circulation des services. Les dispositions attaquées imposent des obligations purement administratives aux prestataires de services de communications électroniques. Ces obligations ne menacent en aucune façon les activités des opérateurs étrangers sur le territoire belge.

A.19.2. À titre subsidiaire, le Conseil des ministres fait valoir que la restriction dénoncée qui est apportée à la libre circulation des services est appropriée au regard de la lutte contre la criminalité grave et le terrorisme, et se trouve dans un rapport raisonnable de proportionnalité par rapport à cet objectif. Un tel objectif constitue un motif impérieux d'intérêt général qui permet de restreindre la libre circulation des services. L'identification de criminels et de terroristes sur la base du trafic de leurs données mobiles est nécessaire et adéquate dans l'optique d'une lutte efficace contre ces phénomènes. Le simple fait qu'il n'existe pas en la matière de législation harmonisée au niveau européen ne suffit pas pour remettre en cause la pertinence des mesures attaquées au regard de l'objectif poursuivi.

Le Conseil des ministres souligne que la Cour de justice accepte généralement les restrictions apportées à la libre circulation des services qui découlent de mesures administratives. Ainsi, elle a déjà accepté que l'on impose à des entreprises commercialisant des signaux d'émission et de télévision numérique de s'inscrire sur un registre

national ou que l'on impose à des entreprises du secteur de la construction de conserver des documents sociaux et de travail dans l'État membre d'accueil.

A.20.1. Compte tenu de la formulation générale de l'article 56 du Traité sur le fonctionnement de l'Union européenne, les parties requérantes estiment que des obligations purement administratives constituent également une entrave à la libre prestation de services. L'obligation imposée entraîne en effet des charges administratives et financières supplémentaires qui peuvent dissuader les prestataires de services de proposer des services de communications électroniques en Belgique. Cette charge administrative a d'ailleurs été reconnue dans les travaux préparatoires.

A.20.2. Le ministre de la Justice a d'ailleurs indiqué, lors de la séance plénière du 18 juin 2015, avoir commandé une étude sur la suppression des cartes anonymes prépayées parce que les opérateurs craignaient que cette mesure augmente les lourdeurs administratives. Cette étude, qui n'a pas été communiquée par le Conseil des ministres, semble pertinente pour apprécier l'entrave à la libre prestation de services parce qu'elle pourrait révéler les données nécessaires pour évaluer le caractère approprié et proportionnel des dispositions attaquées. C'est la raison pour laquelle les parties requérantes demandent que la Cour décide, conformément à l'article 91, 2°, de la loi spéciale du 6 janvier 1989 sur la Cour constitutionnelle, que le Conseil des ministres doit mettre cette étude à disposition.

A.21. Le Conseil des ministres constate que les parties requérantes n'invoquent aucun élément laissant apparaître que les dispositions attaquées imposent de lourdeurs administratives telles qu'elles dissuaderaient des opérateurs étrangers de proposer des services de communications électroniques en Belgique.

En outre, il ressort de l'article 130 de la loi du 13 juin 2005 qu'un anonymat limité demeure possible. Conformément à cette disposition, les opérateurs doivent en effet permettre gratuitement que le numéro d'appelant de l'utilisateur final reste anonyme pour le destinataire de la communication.

A.22. Les parties requérantes allèguent dans leur mémoire complémentaire que l'arrêt de la Cour n° 57/2021 du 22 avril 2021 n'est pas pertinent pour apprécier la deuxième branche du deuxième moyen.

La troisième branche du deuxième moyen

A.23. Dans la troisième branche du deuxième moyen, les parties requérantes dénoncent le fait que l'obligation d'identification instaurée par les dispositions attaquées représente une restriction injustifiée à la liberté de recevoir ou de communiquer des informations ou des idées et au secret des sources journalistiques.

A.24. La liberté d'expression implique la liberté de rechercher, de recevoir et de transmettre des informations et des idées de quelque nature que ce soit, sans limite, oralement ou sous forme écrite ou imprimée ou sous forme artistique ou à l'aide d'autres médias au choix.

Comme les dispositions attaquées instaurent une obligation d'identification généralisée et indifférenciée pour tous les utilisateurs finaux de services de communications électroniques, elle limite la liberté d'expression. Il ressort en effet de la jurisprudence de la Cour de justice que l'obligation de conservation de données de communications est de nature à avoir une incidence sur l'exercice, par les utilisateurs de services de communications électroniques, de leur liberté d'expression.

Le traitement des données d'identification visées par les dispositions attaquées, effectué en vertu de la loi du 29 mai 2016, permet d'établir un profil de la personnalité de chaque citoyen et de suivre ses mouvements. Les lanceurs d'alerte seront donc freinés dans leurs contacts avec des personnalités politiques et des journalistes pour rendre publiques des informations se rapportant à des pratiques frauduleuses. L'enregistrement de telles personnes en tant qu'utilisateurs finaux de services de communications électroniques a donc une incidence directe sur le flux d'informations en direction de la presse et de la classe politique.

En outre, l'impossibilité pour les journalistes et les personnalités politiques de prendre connaissance de façon anonyme d'informations socialement importantes excède les limites du strict nécessaire au regard de ces objectifs. Cette impossibilité remet effectivement en cause des mécanismes de contrôle démocratiques essentiels.

A.25.1. Selon le Conseil des ministres, les parties requérantes n'ont pas d'intérêt à soulever cette branche puisqu'elles ne sont pas journalistes. Par ailleurs, cette branche ne vise pas tant les dispositions attaquées que la loi du 29 mai 2016.

A.25.2. Sur le fond, l'objectif des dispositions attaquées n'est pas de museler la liberté de la presse, d'autant plus que le secret des sources du journaliste ne sera levé que pour contrer une menace d'atteinte à l'intégrité physique de personnes. Le secret des sources ne peut pas être levé s'il y a déjà eu atteinte à l'intégrité physique de personnes. Comme les dispositions attaquées s'inscrivent dans le cadre de la recherche et de la poursuite de la criminalité grave, elles ne seront donc pas appliquées pour contourner le secret des sources. Pour autant qu'il se produise quand même une situation imposant de lever le secret des sources d'un journaliste pour protéger l'intégrité physique de tiers, une telle levée se justifie, au vu de la jurisprudence de la Cour, en raison de la gravité et du caractère souvent irréparable des infractions qui constituent une atteinte grave à l'intégrité physique.

A.26.1. Les parties requérantes estiment avoir effectivement intérêt à la troisième branche du deuxième moyen, étant donné que la liberté d'expression garantit le droit de quiconque de recevoir et de transmettre des informations ou des idées. De plus, les parties requérantes sont tous des conseillers communaux de la commune de Brecht qui, dans le cadre de leurs activités politiques, veulent pouvoir appeler de manière anonyme.

Il est par ailleurs inexact de prétendre que la branche du moyen porte sur la loi du 29 mai 2016. C'est la loi attaquée qui supprime l'anonymat de la carte prépayée et qui empêche les parties requérantes de continuer à utiliser des services de communications électroniques de manière anonyme.

A.26.2. Sur le fond, les parties requérantes soulignent que la loi attaquée supprime l'anonymat de la carte prépayée vis-à-vis de tous les utilisateurs finaux, sans prévoir une exception pour les journalistes. Le secret des sources des journalistes est donc limité dans tous les cas.

A.27. Les parties requérantes soulignent dans leur mémoire complémentaire que, par son arrêt du 6 octobre 2020 en cause *La Quadrature du Net e.a.* (C-511/18), la Cour de justice a qualifié de restriction de la liberté d'expression et de communication la transmission des données de trafic et de localisation et elle a ajouté que ce constat vaut en particulier pour les personnes dont les communications sont soumises au secret professionnel ainsi qu'aux journalistes et aux lanceurs d'alerte. La multitude de données conservées peut effectivement produire un effet dissuasif sur les activités de ces personnes. Selon les parties requérantes, le même raisonnement s'applique aux simples données d'identification.

Quant au troisième moyen

A.28. Dans leur troisième moyen, les parties requérantes font valoir que l'article 2 de la loi attaquée n'est pas compatible avec les articles 10, 11, 12 et 14 de la Constitution, lus en combinaison avec les articles 6 et 7 de la Convention européenne des droits de l'homme, avec les articles 48, 49 et 52 de la Charte des droits fondamentaux de l'Union européenne, avec le principe général du droit à un procès équitable et du droit de défense, en ce compris la présomption d'innocence, et avec le principe de légalité en matière pénale.

La présomption d'imputabilité instaurée par la disposition attaquée, en vertu de laquelle la personne physique ou morale identifiée est, jusqu'à preuve du contraire, responsable de l'utilisation du service de communications électroniques qui lui est fourni, n'est pas proportionnée à l'objectif d'éviter la transmission de cartes prépayées à des tiers.

A.29.1. La présomption d'imputabilité viole le principe de légalité en matière pénale étant donné que sa portée est incertaine. Il est impossible de déterminer s'il s'agit d'une responsabilité contractuelle vis-à-vis de l'opérateur, d'une responsabilité aquilienne vis-à-vis des tiers, ou d'une responsabilité pénale. La seule réponse donnée à ce grief dans l'exposé des motifs est que la présomption d'imputabilité doit empêcher qu'une personne s'identifie à la place d'un tiers qui utilise réellement le service de communications électroniques, pour dissimuler ainsi l'identité de ce tiers. Du fait de sa formulation vague, la disposition attaquée ne clarifie pas, mais n'exclut pas non plus, que la présomption d'imputabilité puisse déterminer la responsabilité pénale de l'utilisateur final identifié.

A.29.2. Une telle présomption d'imputabilité n'est pas raisonnablement proportionnée à l'objectif poursuivi. La disposition attaquée n'empêche pas l'achat d'une carte prépayée à la demande d'un tiers ou la revente ultérieure de cette carte à un tiers. L'article 5 de l'arrêté royal du 27 novembre 2016 prévoit la possibilité de céder une carte prépayée à certains tiers. Mais, d'autre part, un téléphone peut aussi être volé, ou des tiers peuvent, sous de faux prétextes, inciter des utilisateurs finaux de bonne foi à mettre leur téléphone à leur disposition.

Le champ d'application de la présomption d'imputabilité n'est d'ailleurs pas limité à des infractions terroristes ou à des formes graves de criminalité. Il s'avère que la présomption s'applique à toutes les infractions. Il est dès lors impossible pour les utilisateurs finaux de savoir quels actes ou négligences mettent leur responsabilité pénale en cause. Pourtant, un utilisateur final qui met de bonne foi sa carte prépayée à la disposition d'un tiers est dans l'impossibilité de savoir quels faits ce tiers a l'intention de commettre. Il ne peut pas non plus contrôler l'utilisation effectuée par ce tiers, étant donné que cela est punissable en vertu de l'article 124 de la loi du 13 juin 2005 et de l'article 314*bis* du Code pénal.

A.29.3. La présomption d'imputabilité implique également que l'utilisateur final qui laisse l'auteur d'une infraction terroriste utiliser sa carte prépayée, pourra être lui-même poursuivi sur la base des articles 140 et 141 du Code pénal. S'il ne parvient pas à fournir la preuve contraire, il sera en effet condamné pénalement pour la mise à disposition de moyens de communication aux fins de commettre des infractions terroristes.

A.29.4. On peut raisonnablement penser que la preuve contraire prévue par la loi attaquée ne pourra être rapportée, étant donné que l'utilisateur final identifié est dans l'impossibilité d'être au courant de l'utilisation faite par le tiers du service de communications électroniques.

A.30.1. Selon le Conseil des ministres, il est impossible qu'une présomption réfragable puisse violer la présomption d'innocence. D'ailleurs, la disposition attaquée ajoute peu de choses au postulat qui s'applique à chaque instruction, à savoir que l'utilisateur d'une ligne téléphonique est à l'origine de la communication. Il en va de même pour l'utilisation de lignes fixes ou pour l'utilisation d'abonnements. La disposition attaquée ne porte pas non plus atteinte à la présomption d'innocence, étant donné qu'elle n'empêche pas que l'intéressé soit présumé innocent jusqu'à preuve du contraire. Si l'utilisateur peut démontrer de façon crédible qu'il n'a pas utilisé son moyen de communication au moment des faits, il ne peut pas être condamné. Selon la jurisprudence constante de la Cour de cassation, le prévenu doit échapper aux poursuites si son explication est matériellement possible et n'est pas contredite par les pièces du dossier.

La Cour constitutionnelle juge que les présomptions légales ne sont en principe pas contraires à la présomption d'innocence, pour autant qu'elles soient raisonnablement proportionnées à un objectif légitime, en prenant en compte la gravité de l'enjeu et en préservant les droits de la défense.

A.30.2. Selon le Conseil des ministres, la disposition attaquée n'impose elle-même aucune sanction pénale. La transmission d'une carte prépayée à des tiers n'est donc pas sanctionnée pénalement. La référence faite par les parties requérantes au principe de légalité en matière pénale et au principe de proportionnalité de la peine est donc dénuée de toute pertinence.

A.31. Les parties requérantes estiment que c'est à la Cour, et non au Conseil des ministres, qu'il appartient de juger la façon d'interpréter la disposition attaquée. Il s'avère en tout cas que la portée de la disposition attaquée est incertaine et qu'elle est donc difficilement conciliable avec le principe de légalité en matière pénale. Il semble que la disposition attaquée introduise non seulement une présomption d'utilisation, mais aussi une présomption de culpabilité, ce qui constitue donc un renversement de la charge de la preuve. Cette présomption déroge au principe selon lequel la charge de la preuve en matière pénale incombe à la partie poursuivante.

A.32. Selon les parties requérantes, l'arrêt de la Cour n° 57/2021 du 22 avril 2021 ne change rien à la compétence du procureur du Roi ou du juge d'instruction d'identifier l'abonné ou l'utilisateur habituel d'un service de communications électroniques. La présomption d'imputabilité qui est attaquée demeure par conséquent pertinente.

Quant au quatrième moyen

A.33. Dans leur quatrième moyen, les parties requérantes font valoir que l'article 3 de la loi attaquée n'est pas compatible avec les articles 10, 11 et 22 de la Constitution, lus en combinaison avec l'article 8 de la Convention européenne des droits de l'homme, avec les articles 7, 8 et 52 de la Charte des droits fondamentaux de l'Union européenne, avec les articles 2, point a), 6, 13 et 22 de la directive 95/46/CE et avec les articles 1er, 2, 3, 5, 6, 9 et 15 de la directive 2002/58/CE. Le moyen se subdivise en cinq branches.

A.34.1. Dans la première branche du quatrième moyen, les parties requérantes font valoir que l'accès, par les services de renseignement et de sécurité, aux données d'identification collectées et conservées en vertu de la loi attaquée, constitue une limitation injustifiée de la protection de la vie privée.

A.34.2. La disposition attaquée permet aux services de renseignement et de sécurité de requérir le concours d'une banque ou d'une institution financière pour procéder à l'identification de l'utilisateur final d'une carte prépayée. Il s'agit donc d'un accès à des données à caractère personnel qui sont traitées en vertu de la loi du 29 mai 2016. Une telle procédure constitue une ingérence dans le droit au respect de la vie privée et familiale.

Il ressort de la jurisprudence de la Cour de justice qu'une telle limitation doit reposer sur l'un des objectifs énumérés limitativement par l'article 15, paragraphe 1, première phrase, de la directive 2002/58/CE. Les objectifs liés à la lutte contre des infractions ne peuvent porter, compte tenu de la nature des principes en cause, que sur des crimes graves. En outre, l'accès aux données à caractère personnel traitées ne peut excéder les limites du strict nécessaire pour atteindre cet objectif. Enfin, le cadre législatif doit fixer les conditions matérielles et procédurales de l'accès, ainsi que prévoir des garanties adéquates pour empêcher une utilisation abusive de ces données. Le respect de ces conditions doit faire l'objet d'un contrôle préalable par une juridiction ou une autorité administrative indépendante.

A.34.3. Selon les parties requérantes, l'article 16/2, §§ 2 à 4, de la loi du 30 novembre 1998 « organique des services de renseignement et de sécurité » n'offre pas suffisamment de garanties. Il soumet l'identification de l'utilisateur final de cartes prépayées à la méthode ordinaire de collecte de données. Il s'ensuit que ces données peuvent être utilisées par les services de renseignement et de sécurité chaque fois que cette utilisation est dans l'intérêt de l'exercice de leurs missions. Ils peuvent donc demander d'avoir accès aux données collectées et, pour ce faire, requérir au besoin le concours d'une banque ou d'une institution financière, indépendamment de l'existence d'une menace terroriste et indépendamment de la lutte contre la criminalité grave.

En outre, la disposition attaquée ne limite pas l'accès aux données d'identification de l'utilisateur final aux personnes soupçonnées de crimes graves ou d'activités terroristes. Elle n'énumère pas non plus les éléments objectifs pouvant justifier un accès à ces données. Elle excède donc les limites du strict nécessaire au regard de la sécurité nationale, de la sûreté de l'État, de la sécurité publique et de la lutte contre la criminalité grave.

A.35.1. Dans la deuxième branche du quatrième moyen, les parties requérantes font valoir que l'accès des services de renseignement et de sécurité aux données d'identification collectées et conservées en vertu de la loi attaquée n'est pas compatible avec le droit à la protection de la vie privée, en ce que l'accès aux données conservées n'est pas subordonné à un contrôle préalable de la part d'une juridiction ou d'une autorité administrative indépendante.

A.35.2. L'article 16/2, § 2, de la loi du 30 novembre 1998, modifié par la disposition attaquée, ne soumet pas à un contrôle judiciaire la réquisition par les services de renseignement et de sécurité du concours d'une banque ou d'une institution financière pour identifier l'utilisateur final d'une carte prépayée. En effet, celle-ci est effectuée par le dirigeant du service ou son délégué. Il s'agit en principe de l'administrateur général de la Sûreté de l'État. La demande n'est pas soumise à un avis conforme préalable de la commission administrative chargée de la surveillance des méthodes spécifiques et exceptionnelles de recueil de données par les services de renseignement et de sécurité, créée par l'article 43/1 de la loi du 30 novembre 1998. Il n'est pas non plus prévu le moindre contrôle judiciaire préalable.

A.36.1. Dans la troisième branche du quatrième moyen, les parties requérantes font valoir que l'accès des services de renseignement et de sécurité aux données d'identification collectées et conservées en vertu de la loi attaquée n'est pas compatible avec le droit à la protection de la vie privée, en ce que la disposition attaquée ne prévoit pas de conditions matérielles et procédurales pour l'accès aux données conservées.

A.36.2. La disposition attaquée indique seulement que l'accès aux données d'identification conservée s'effectue « sur réquisition » et que cette réquisition doit être introduite par écrit, sauf en cas d'urgence. La réquisition ne doit pas être motivée. La nature des données demandées n'est pas non plus explicitée. La disposition attaquée ne précise pas non plus les conditions matérielles et procédurales auxquelles la réquisition doit satisfaire. Des pressions sont toutefois exercées sur les banques et institutions financières pour qu'elles répondent favorablement à cette réquisition, puisqu'elles risquent en cas de refus une amende de vingt-six euros à dix mille euros, majorée des décimes additionnels, conformément à l'article 16/2, § 3, de la loi du 30 novembre 1998.

A.37. Dans la quatrième branche du quatrième moyen, les parties requérantes font valoir que l'accès des services de renseignement et de sécurité aux données d'identification collectées et conservées en vertu de la loi attaquée n'est pas compatible avec le droit à la protection de la vie privée, en ce que la disposition attaquée ne prévoit pas que les services de renseignement et de sécurité qui ont eu accès aux données à caractère personnel traitées doivent en informer l'utilisateur final concerné, et en ce qu'elle ne prévoit pas de contrôle juridictionnel effectif, en fait comme en droit, sur la légalité de cet accès.

A.38. Dans la cinquième branche du quatrième moyen, les parties requérantes font valoir que l'accès des services de renseignement et de sécurité aux données d'identification collectées et conservées en vertu de la loi attaquée n'est pas compatible avec le droit à la protection de la vie privée, en ce que la disposition attaquée n'exclut pas que des services de renseignement et de sécurité étrangers aient accès aux données d'identification conservées. L'article 20 la loi du 30 novembre 1998 rend même un tel échange de données à caractère personnel explicitement possible. Cette disposition n'établit aucune distinction selon la nature des données communiquées ou leur utilité pour des enquêtes en cours.

A.39.1. Le Conseil des ministres estime que les cinq branches du quatrième moyen peuvent en fait se réduire à une seule question de droit. Ce moyen n'est d'ailleurs pas recevable en ce qu'il demande à la Cour d'évaluer la disposition attaquée au regard des directives 95/46/CE et 2002/58/CE.

Il s'avère en tout cas que l'accès des services de sécurité et de renseignement à certaines données bancaires, en l'occurrence aux données permettant d'identifier l'utilisateur final d'une carte prépayée, ne se rapporte pas à des données à caractère personnel, de sorte que la directive 2002/58/CE ne s'applique pas. En effet, l'article 1, paragraphe 1, de la directive 2002/58/CE et l'article 3, paragraphe 1, de la directive 95/46/CE prévoient que ces directives ne s'appliquent pas au traitement de données à caractère personnel issues d'activités de la sûreté de l'État, de la défense, de la sécurité publique, et de la prévention, la recherche, la détection et la poursuite d'infractions pénales ou de manquements à la déontologie dans le cas des professions réglementées.

La disposition attaquée fait partie du droit pénal et du droit de la procédure pénale, de la sécurité publique et de la protection et de la sûreté de l'État. Ces matières ne relèvent pas du champ d'application du droit de l'Union européenne.

A.39.2. Selon le Conseil des ministres, la référence des parties requérantes à la jurisprudence de la Cour de justice est hors de propos. L'arrêt de la Cour de justice du 21 décembre 2016 en cause *Tele2 Sverige* (C-203/15 et C-698/15) portait en effet sur des données de trafic et de localisation, alors que l'article 16/2 de la loi du 30 novembre 1998 porte uniquement sur des données d'identification.

Même s'il fallait étendre l'enseignement de cet arrêt, force est de constater que l'éventuelle ingérence dans la vie privée et familiale est beaucoup plus limitée lorsque de simples données d'identification sont en cause. En soi, ces données ne permettent en effet pas de déterminer la source, le destinataire, la date, le moment, la durée et la nature d'une communication. Il n'est pas non plus possible de déterminer la fréquence des communications entre deux personnes sur la base de ces données. Les simples données d'identification ne permettent donc pas de tirer des conclusions précises sur la vie privée des personnes dont les données sont conservées, comme leurs habitudes quotidiennes, leur résidence permanente ou temporaire, leurs déplacements journaliers ou autres, les activités qu'elles exercent, leurs relations sociales ou les milieux qu'elles fréquentent.

La question est donc de savoir si la simple réquisition du concours d'une banque ou d'une institution financière pour procéder à l'identification de l'utilisateur final d'une carte prépayée est effectivement constitutive d'une ingérence dans la vie privée et familiale.

A.39.3. Enfin, la loi du 30 novembre 1998 énonce suffisamment de garanties pour protéger la vie privée. C'est la raison pour laquelle la réquisition doit être signée par le chef du service ou son délégué. En outre, le service

de la Sûreté de l'État doit conserver une liste de toutes les identifications requises et doit transmettre chaque mois au Comité R une liste des données réclamées. Ces garanties suffisent au regard de l'ingérence très limitée dans la vie privée et familiale qui peut résulter de la disposition attaquée.

A.40.1. Selon les parties requérantes, la directive 2002/58/CE est d'application puisqu'elle porte sur tous les traitements de données à caractère personnel dans le cadre de la fourniture de services de communications électroniques accessibles au public, ainsi que sur toute personne pouvant ainsi être identifiée indirectement ou directement. Cette directive n'établit aucune distinction en fonction de la matière.

Étant donné que les opérateurs sont tenus d'enregistrer la référence des transactions bancaires à l'aide desquelles la carte prépayée est achetée et que les services de renseignement et de sécurité peuvent se procurer un accès à ces données, il s'agit d'un traitement de données à caractère personnel dans le cadre de services de communications électroniques, de sorte que la directive 2002/58/CE est d'application.

A.40.2. Selon les parties requérantes, la distinction opérée par le Conseil des ministres entre des données de trafic et de localisation, d'une part, et de simples données d'identification, d'autre part, n'est pas pertinente. La seule chose importante est que des données à caractère personnel sont traitées pour garantir la sûreté de l'État, sans que les autorités nationales y aient accès. En ce sens, la référence à l'arrêt précité de la Cour de justice du 21 décembre 2016 est bel et bien pertinente.

En outre, les données d'identification conservées ne peuvent pas être dissociées des données de localisation et de communication conservées. En effet, dès l'instant où une autorité a identifié un utilisateur final d'un service de communications électroniques en vertu de la loi attaquée, elle peut relier elle-même ces données aux autres données à caractère personnel de l'intéressé qui sont traitées, parmi lesquelles ses données de localisation et de communication. L'identification de l'utilisateur final constitue donc une première étape dans l'ingérence excessive dans la vie privée et familiale telle qu'elle a été décrite par le Conseil des ministres.

A.40.3. Les trois garanties énumérées par le Conseil des ministres ne suffisent nullement au regard d'une telle limitation du droit au respect de la vie privée et familiale, comme en atteste également la jurisprudence précitée de la Cour de justice de l'Union européenne. Pour être conforme à cette jurisprudence, la loi attaquée aurait dû préciser que l'accès aux données conservées ne peut être accordé que dans le cadre de la lutte contre la criminalité grave, elle aurait dû soumettre cet accès à l'avis préalable d'une juridiction ou d'une commission administrative indépendante, elle aurait dû régler les conditions matérielles et procédurales de cet accès, elle aurait dû stipuler que les utilisateurs finaux identifiés doivent être informés de tout accès à leurs données d'identification et qu'il faut leur accorder dans ce cadre un accès effectif au juge, et elle aurait dû prévoir que les données d'identification ne peuvent être échangées avec des services de renseignement et de sécurité étrangers.

A.41. Le Conseil des ministres souligne que la disposition attaquée ne se rapporte pas à des données d'identification, mais à l'accès à des données bancaires. Les normes de contrôle mentionnées dans le moyen, et à tout le moins les directives 95/46/CE et 2002/58/CE mentionnées dans le même moyen, ne s'y appliquent pas.

Le fait que l'utilisateur final n'est pas informé du traitement de ses données à caractère personnel et de l'accès à celles-ci s'explique par la particularité du travail des services de renseignement et de sécurité, qui consiste à garantir la sûreté de l'État, notamment pour prévenir des attentats terroristes. Ces services n'ont aucune finalité judiciaire, et les données à caractère personnel traitées ne sont pas utilisées en matière pénale.

A.42. Les parties requérantes soulignent dans leur mémoire en réponse que l'arrêt n° 57/2021 du 22 avril 2021 n'a pas modifié les règles en matière d'accès des services de renseignement et de sécurité aux données d'identification conservées. L'arrêt de la Cour de justice du 6 octobre 2020 en cause *La Quadrature du Net e.a.* (C-511/18) n'a pas d'incidence non plus sur le quatrième moyen.

Selon elles, il convient toutefois de renvoyer à l'arrêt de la Cour de justice du 2 mars 2021 en cause *Prokuratuur* (C-746/18), par lequel la Cour de justice a défini ce qu'il y a lieu d'entendre par l'« autorité administrative indépendante » qui doit assurer le contrôle préalable quant à l'accès des services de renseignement et de sécurité aux données à caractère personnel traitées. Cette instance doit être compétente pour concilier tous les intérêts et droits concernés et doit pouvoir exercer ses tâches de manière objective et impartiale, en étant libre de toute influence extérieure.

Dès lors que l'article 16/2, § 2, de la loi du 30 novembre 1998 ne requiert qu'une autorisation du dirigeant du service ou de son délégué, sans autorisation préalable de la commission BIM, il ne saurait s'agir, en l'espèce, d'une autorité administrative indépendante. En outre, la disposition attaquée ne garantit pas que l'accès des services de renseignement et de sécurité aux données à caractère personnel traitées reste limité aux cas où des intérêts vitaux de sécurité nationale, de défense nationale ou de sécurité publique sont en jeu.

Elle ne garantit pas non plus que la personne concernée ait connaissance de cet accès afin qu'elle puisse exercer son droit au contrôle juridictionnel. Par l'arrêt n° 41/2019 du 14 mars 2019, la Cour a cependant obligé le législateur à prévoir un mécanisme de notification active par lequel la personne concernée est informée du fait qu'elle a fait l'objet d'une méthode de surveillance secrète par les services de sécurité et de renseignement.

Enfin, les parties requérantes soulignent que la transmission mensuelle au Comité R de la liste des données requises a été supprimée par la loi du 30 mars 2017. Cette garantie, à laquelle renvoie le Conseil des ministres, a donc disparu.

Quant au maintien des effets

A.43. Enfin, les parties requérantes soulignent dans leur mémoire complémentaire que, par l'arrêt du 6 octobre 2020 en cause *La Quadrature du Net e.a.* (C-511/18), la Cour de justice a jugé que la Cour constitutionnelle devait annuler les dispositions législatives qui étaient contraires à cet arrêt, sans être autorisée à en maintenir les effets. Par conséquent, les effets de la loi attaquée ne peuvent pas être maintenus non plus.

- *B* -

B.1.1. La loi du 1er septembre 2016 « portant modification de l'article 127 de la loi du 13 juin 2005 relative aux communications électroniques et de l'article 16/2 de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité » (ci-après : la loi attaquée) dispose :

« CHAPITRE 1er. - Objet

Article 1er. La présente loi règle une matière visée à l'article 74 de la Constitution.

CHAPITRE 2. - Modifications de la loi du 13 juin 2005 relative aux communications électroniques

Art. 2. Dans l'article 127 de la loi du 13 juin 2005 relative aux communications électroniques, modifié par les lois des 4 février 2010, 10 juillet 2012, 27 mars 2014 et 29 mai 2016, les modifications suivantes sont apportées :

1° dans le paragraphe 1er, les modifications suivantes sont apportées :

a) dans l'alinéa 1er, les mots ' aux canaux de vente de services de communications électroniques, aux entreprises fournissant un service d'identification ' sont insérés entre les mots ' visés à l'article 126, § 1er, alinéa 1er, ' et les mots ' ou aux utilisateurs finals ';

b) dans le texte néerlandais, à l'alinéa 1er, les mots ' de verkoopkanalen van elektronische-communicatiediensten, de ondernemingen die een identificatiedienst verstrekken ' sont insérés entre les mots ' bedoeld in artikel 126, § 1, eerste lid, ' et les mots ' of aan de eindgebruikers ';

c) sept alinéas rédigés comme suit sont insérés entre les alinéas 1er et 2 :

' Pour ce qui concerne l'identification de l'utilisateur final, l'opérateur ou le fournisseur visé à l'article 126, § 1er, alinéa 1er, est le responsable du traitement au sens de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel.

Sauf preuve contraire, la personne identifiée est présumée utiliser elle-même le service de communications électroniques.

Lorsque l'utilisateur final présente un document d'identification comprenant le numéro de registre national, l'opérateur, le fournisseur visé à l'article 126, § 1er, alinéa 1er, le canal de vente de services de communications électroniques ou l'entreprise fournissant un service d'identification collecte ce numéro.

Le canal de vente de services de communications électroniques ne conserve pas de données ou de documents d'identification, qui sont transmis à l'opérateur, au fournisseur visé à l'article 126, § 1er, alinéa 1er ou à l'entreprise fournissant un service d'identification.

Si une introduction directe dans les systèmes informatiques de l'opérateur, du fournisseur visé à l'article 126, § 1er, alinéa 1er ou de l'entreprise fournissant un service d'identification n'est pas possible, le canal de vente de services de communications électroniques peut faire une copie du document d'identification, dont la carte d'identité électronique belge, mais cette copie est détruite au plus tard après l'activation du service de communications électroniques.

L'opérateur ou le fournisseur visé à l'article 126, § 1er, alinéa 1er conserve une copie des documents d'identification autres que la carte d'identité électronique belge.

Les données et documents d'identification collectés sont conservés conformément à l'article 126, § 3, alinéa 1er. '

2° le paragraphe 3 est complété par l'alinéa suivant :

' Les utilisateurs finals non identifiés de cartes prépayées achetées avant l'entrée en vigueur de l'arrêté royal visé au paragraphe 1er, qui sont définis par cet arrêté royal, s'identifient dans le délai fixé par l'opérateur ou le fournisseur visé à l'article 126, § 1er, alinéa 1er, ce délai ne pouvant excéder six mois après la publication de l'arrêté royal visé au paragraphe 1er. L'interdiction visée au paragraphe 2 ne s'applique qu'après la fin du délai accordé à l'utilisateur final pour s'identifier. '

3° dans le paragraphe 4, les modifications suivantes sont apportées :

a) les mots ‘ ou un fournisseur visé à l’article 126, § 1er, alinéa 1er, ’ sont insérés entre les mots ‘ un opérateur ’ et les mots ‘ ne respecte pas les mesures techniques et administratives qui lui sont imposées ’;

b) dans le texte néerlandais, les mots ‘ binnen de door de Koning vastgestelde termijn ’ sont abrogés;

c) dans le texte néerlandais, les mots ‘ of een aanbieder bedoeld in artikel 126, § 1, eerste lid, ’ sont insérés entre les mots ‘ een operator ’ et les mots ‘ niet voldoet aan de hem opgelegde technische en administratieve maatregelen ’;

d) les mots ‘ dans le délai fixé ’ sont remplacés par les mots ‘ par le présent article ou ’;

e) dans le texte néerlandais, les mots ‘ door dit artikel of door de Koning ’ sont insérés entre les mots ‘ niet voldoen aan de hen ’ et les mots ‘ opgelegde technische en administratieve maatregelen ’;

4° dans le paragraphe 5, les modifications suivantes sont apportées :

a) dans l’alinéa 1er, les mots ‘ et les fournisseurs visés à l’article 126, § 1er, alinéa 1er, ’ sont insérés entre les mots ‘ Les opérateurs ’ et les mots ‘ déconnectent les utilisateurs finals ’;

b) dans le texte néerlandais, dans l’alinéa 1er, les mots ‘ en de aanbieders bedoeld in artikel 126, § 1, eerste lid, ’ sont insérés entre les mots ‘ De operatoren ’ et les mots ‘ sluiten de eindgebruikers ’;

c) dans l’alinéa 1er, les mots ‘ dans le délai fixé ’ sont remplacés par les mots ‘ par le présent article ou ’;

d) dans le texte néerlandais, à l’alinéa 1er, les mots ‘ binnen de door de Koning vastgestelde termijn ’ sont abrogés;

e) dans le texte néerlandais, à l’alinéa 1er, les mots ‘ door dit artikel of door de Koning ’ sont insérés entre les mots ‘ niet voldoen aan de hen ’ et les mots ‘ opgelegde technische en administratieve maatregelen ’;

f) l’alinéa 2 est abrogé.

CHAPITRE 3. - Modifications de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité

Art. 3. Dans l’article 16/2 de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité, inséré par la loi du 5 février 2016, les modifications suivantes sont apportées :

1° les actuels alinéas 1er à 4 formeront le paragraphe 1er et le mot ‘ chef ’ est chaque fois remplacé par le mot ‘ dirigeant ’;

2° il est inséré un paragraphe 2, rédigé comme suit :

‘ § 2. Les services de renseignement et de sécurité peuvent, dans l’intérêt de l’exercice de leurs missions, requérir le concours d’une banque ou d’une institution financière pour procéder à l’identification de l’utilisateur final d’une carte prépayée visée dans l’article 127 de la loi du 13 juin 2005 relative aux communications électroniques, sur la base de la référence d’une transaction bancaire électronique qui est liée à la carte prépayée et qui a préalablement été communiquée par un opérateur ou un fournisseur en application du paragraphe 1er.

La réquisition est effectuée par écrit par le dirigeant de service ou son délégué. En cas d’urgence, le dirigeant de service ou son délégué peut requérir ces données verbalement. Cette réquisition verbale est confirmée dans un délai de vingt-quatre heures par une réquisition écrite.

Toute banque et toute institution financière qui est requise donne sans délai au dirigeant de service ou à son délégué les données qui ont été demandées.

Les données d’identification que les services de renseignement et de sécurité reçoivent dans le cadre de l’exercice de la méthode visée au présent paragraphe, se limitent aux données d’identification visées au paragraphe 1er. ’;

3° l’actuel alinéa 5 formera le paragraphe 3;

4° dans le texte néerlandais, dans l’actuel sixième alinéa, dont le texte formera le paragraphe 4, les mots ‘ de betrokken inlichtingen- en veiligheidsdiensten ’ sont remplacés par les mots ‘ de betrokken inlichtingen- en veiligheidsdienst ’ et dans le texte français, les mots ‘ et de sécurité ’ sont insérés entre les mots ‘ service de renseignement ’ et le mot ‘ concerné ’ ».

B.1.2. La loi attaquée fait partie des mesures de lutte contre le terrorisme qui ont été prises à la suite des attentats terroristes commis à Paris le 13 novembre 2015 et à Bruxelles le 22 mars 2016 (*Doc. parl.*, Chambre, 2015-2016, DOC 54-1964/001, p. 2). L’article 2 de la loi attaquée modifie l’article 127 de la loi du 13 juin 2005 « relative aux communications électroniques » (ci-après : la loi du 13 juin 2005) en vue de la suppression de l’anonymat des cartes de téléphonie mobile prépayées. L’article 3 de la loi attaquée modifie l’article 16/2 de la loi du 30 novembre 1998 « organique des services de renseignement et de sécurité » (ci-après : la loi du 30 novembre 1998) afin de permettre l’identification de l’utilisateur final d’une carte de téléphonie mobile prépayée sur la base de la transaction bancaire en ligne qui a été effectuée pour l’acheter.

B.2.1. L'article 127 de la loi du 13 juin 2005, modifié par l'article 2 de la loi attaquée, dispose :

« § 1er. Le Roi fixe, après avis de la Commission pour la protection de la vie privée et de l'Institut, les mesures techniques et administratives qui sont imposées aux opérateurs, aux fournisseurs visés à l'article 126, § 1er, alinéa 1er, aux canaux de vente de services de communications électroniques, aux entreprises fournissant un service d'identification ou aux utilisateurs finals, en vue de permettre :

1° l'identification de la ligne appelante dans le cadre d'un appel d'urgence;

2° l'identification de l'utilisateur final, le repérage, la localisation, les écoutes, la prise de connaissance et l'enregistrement des communications privées aux conditions prévues par les articles 46*bis*, 88*bis* et 90*ter* à 90*decies* du Code d'instruction criminelle et par la loi du 30 novembre 1998 organique des services de renseignement et de sécurité.

Pour ce qui concerne l'identification de l'utilisateur final, l'opérateur ou le fournisseur visé à l'article 126, § 1er, alinéa 1er, est le responsable du traitement au sens de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel.

Sauf preuve contraire, la personne identifiée est présumée utiliser elle-même le service de communications électroniques.

Lorsque l'utilisateur final présente un document d'identification comprenant le numéro de registre national, l'opérateur, le fournisseur visé à l'article 126, § 1er, alinéa 1er, le canal de vente de services de communications électroniques ou l'entreprise fournissant un service d'identification collecte ce numéro.

Le canal de vente de services de communications électroniques ne conserve pas de données ou de documents d'identification, qui sont transmis à l'opérateur, au fournisseur visé à l'article 126, § 1er, alinéa 1er ou à l'entreprise fournissant un service d'identification.

Si une introduction directe dans les systèmes informatiques de l'opérateur, du fournisseur visé à l'article 126, § 1er, alinéa 1er ou de l'entreprise fournissant un service d'identification n'est pas possible, le canal de vente de services de communications électroniques peut faire une copie du document d'identification, dont la carte d'identité électronique belge, mais cette copie est détruite au plus tard après l'activation du service de communications électroniques.

L'opérateur ou le fournisseur visé à l'article 126, § 1er, alinéa 1er conserve une copie des documents d'identification autres que la carte d'identité électronique belge.

Les données et documents d'identification collectés sont conservés conformément à l'article 126, § 3, alinéa 1er.

Le Roi fixe, après l'avis de l'Institut, les tarifs rétribuant la collaboration des opérateurs et des fournisseurs visés à l'article 126, § 1er, alinéa 1er, aux opérations visées à l'alinéa 1er, 2° ainsi que le délai dans lequel les opérateurs ou les abonnés doivent donner suite aux mesures imposées.

§ 2. Sont interdites : la fourniture ou l'utilisation d'un service ou d'un équipement qui rend difficile ou impossible l'exécution des opérations visées au § 1er, à l'exception de systèmes d'encryptage qui peuvent être utilisés pour garantir la confidentialité des communications et la sécurité des paiements.

§ 3. Jusqu'à ce que les mesures visées au § 1er entrent en vigueur, l'interdiction visée au § 2 ne s'applique pas aux services de communications électroniques publics mobiles fournis sur la base d'une carte prépayée.

Les utilisateurs finals non identifiés de cartes prépayées achetées avant l'entrée en vigueur de l'arrêté royal visé au paragraphe 1er, qui sont définis par cet arrêté royal, s'identifient dans le délai fixé par l'opérateur ou le fournisseur visé à l'article 126, § 1er, alinéa 1er, ce délai ne pouvant excéder six mois après la publication de l'arrêté royal visé au paragraphe 1er. L'interdiction visée au paragraphe 2 ne s'applique qu'après la fin du délai accordé à l'utilisateur final pour s'identifier.

§ 4. Si un opérateur ou un fournisseur visé à l'article 126, § 1er, alinéa 1er, ne respecte pas les mesures techniques et administratives qui lui sont imposées par le présent article ou par le Roi, il lui est interdit de fournir le service pour lequel les mesures en question n'ont pas été prises.

§ 5. Les opérateurs et les fournisseurs visés à l'article 126, § 1er, alinéa 1er, déconnectent les utilisateurs finals qui ne respectent pas les mesures techniques et administratives qui leur sont imposées par le présent article ou par le Roi, des réseaux et services auxquels les mesures imposées s'appliquent. Ces utilisateurs finals ne sont en aucune manière indemnisés pour la déconnexion ».

B.2.2. L'article 127 de la loi du 13 juin 2005 s'est toujours fondé sur la prémisse selon laquelle tous les utilisateurs finaux de réseaux de communications électroniques doivent être identifiables. À l'origine, cette disposition n'imposait des obligations qu'aux opérateurs, aux fournisseurs et aux utilisateurs finaux de ces services. L'article 127, § 1er, alinéa 1er, confère une habilitation générale au Roi pour fixer les mesures techniques et administratives en vue de permettre cette identifiabilité.

Cette identifiabilité sert deux objectifs. Premièrement, elle vise à contribuer au bon fonctionnement des services d'urgence en permettant l'identification de la ligne appelante d'un appel d'urgence (article 127, § 1er, alinéa 1er, 1°). Deuxièmement, elle contribue au repérage, à la localisation, aux écoutes, à la prise de connaissance et à l'enregistrement des

communications privées aux conditions prévues par les articles 46*bis*, 88*bis* et 90*ter* à 90*decies* du Code d'instruction criminelle et par la loi du 30 novembre 1998 (article 127, § 1er, alinéa 1er, 2°).

L'article 127, § 2, de la loi du 13 juin 2005 interdit la fourniture ou l'utilisation de services ou d'équipements qui rendent l'identifiabilité difficile, à l'exception de systèmes d'encryptage qui peuvent être utilisés pour garantir la confidentialité des communications et la sécurité des paiements.

L'article 127, § 3, de la même loi prévoyait initialement une exception temporaire à cette interdiction pour les utilisateurs finaux de cartes de téléphonie mobile prépayées. Ces utilisateurs finaux étaient dispensés de l'obligation d'être identifiables tant que le Roi n'avait pas encore pris les mesures techniques et administratives visées à l'article 127, § 1er.

B.2.3. L'article 2 de la loi attaquée a modifié l'article 127 de la loi du 13 juin 2005 sur différents points. Premièrement, il en a étendu le champ d'application en imposant certaines des obligations contenues dans cet article également aux canaux de vente de services de communications électroniques et aux entreprises fournissant un service d'identification.

Deuxièmement, cette disposition a ancré dans la loi un certain nombre d'aspects de l'identification de l'utilisateur final. Ainsi, l'opérateur et le fournisseur sont désignés comme les responsables du traitement des données à caractère personnel (article 127, § 1er, alinéa 2). Cette disposition indique également que, sauf preuve contraire, la personne identifiée est présumée utiliser elle-même le service de communications électroniques (article 127, § 1er, alinéa 3), que l'identification doit s'effectuer sur la base d'un document d'identification comportant le numéro de registre national (article 127, § 1er, alinéa 4) et que le canal de vente de services de communications électroniques ne peut pas conserver de copies des données ou des documents d'identification qu'il transmet à l'opérateur (article 127, § 1er, alinéas 5 à 7).

Troisièmement, cette disposition comporte quelques habilitations spécifiques au Roi, telles que l'habilitation conférée au Roi dans le nouvel article 127, § 1er, alinéa 8, de la loi du 13 juin 2005, par laquelle le Roi fixe la rétribution des opérateurs et des fournisseurs dans les cas où ils doivent contribuer à l'identification des utilisateurs finaux de leurs services, ainsi que le

délai dans lequel les opérateurs et les abonnés doivent donner suite aux mesures imposées. Le nouvel alinéa 2 de l'article 127, § 3, de la loi du 13 juin 2005 habilite le Roi à fixer le délai dans lequel l'utilisateur final d'une carte de téléphonie mobile prépayée achetée avant l'entrée en vigueur de la loi attaquée doit s'identifier. Ce délai ne peut pas excéder six mois après la publication de l'arrêté royal visé à l'article 127, § 1er, de la même loi. En vertu du nouvel article 127, § 3, alinéa 2, de la loi du 13 juin 2005, l'anonymat des cartes de téléphonie mobile prépayées n'est levé qu'après la fin de ce délai.

B.2.4. Le Roi a mis à exécution l'article 127 de la loi du 13 juin 2005, du moins pour ce qui concerne les services de communications électroniques qui sont offerts sur la base d'une carte de téléphonie mobile prépayée, par l'arrêté royal du 27 novembre 2016 « relatif à l'identification de l'utilisateur final de services de communications électroniques publics mobiles fournis sur la base d'une carte prépayée » (ci-après : l'arrêté royal du 27 novembre 2016).

L'article 2, 4°, de cet arrêté royal définit le document d'identification valide comme « la carte d'identité belge ou d'un État membre de l'Union européenne, la carte électronique belge pour étrangers, le document reprenant le numéro visé à l'art 8, § 1er, 2°, de la loi du 15 janvier 1990 relative à l'institution et à l'organisation d'une Banque-carrefour de la sécurité sociale ou à l'article 2, alinéa 2, de la loi du 8 août 1983 organisant un registre national des personnes physiques ou le passeport international ou le document officiel remplaçant, à titre provisoire, un des documents susmentionnés qui a été perdu ou volé, pour autant que le document d'identification soit original, lisible et valide ».

Les articles 3 à 6 de l'arrêté royal du 27 novembre 2016 imposent des obligations aux utilisateurs finaux de cartes de téléphonie mobile prépayées. Ils doivent s'identifier auprès de l'opérateur à chaque fois que celui-ci le demande. Lorsqu'ils achètent une nouvelle carte de téléphonie mobile prépayée, ils communiquent leur identité à l'opérateur au plus tard lors de l'activation de cette carte selon une des méthodes d'identification valides. Il leur est en principe interdit de céder leur carte prépayée à des tiers, sauf dans les cas et aux conditions fixés à l'article 5 de l'arrêté royal. S'ils perdent leur carte prépayée ou si celle-ci est volée, ils doivent en informer l'opérateur dans les 24 heures.

Les articles 7 à 9 du même arrêté royal imposent des obligations aux opérateurs. Ces derniers devaient identifier avant le 7 juin 2017 tous les utilisateurs finaux de cartes prépayées qui avaient été achetées avant l'entrée en vigueur, le 17 décembre 2016, de cet arrêté royal. Depuis l'entrée en vigueur de cet arrêté royal, ils ne peuvent plus activer de nouvelles cartes prépayées si l'utilisateur final n'a pas encore été identifié. S'ils sont informés par l'utilisateur final de la perte ou du vol de la carte de téléphonie mobile prépayée, ils doivent la rendre immédiatement inutilisable.

B.2.5. Les articles 9 à 12 du même arrêté royal définissent la manière dont l'utilisateur final d'une carte de téléphonie mobile prépayée doit être identifié et dont ses données d'identification sont traitées. L'opérateur, le fournisseur d'un service d'identification ou le canal de vente de services de communications électroniques collectent ces données en lisant électroniquement la carte d'identité électronique belge ou en faisant un scan, une photo ou une copie de celle-ci, en ce compris de la photo se trouvant sur cette carte et du numéro de cette carte. Avant l'activation de la carte de téléphonie mobile prépayée, l'opérateur doit contrôler si la carte d'identité présentée n'a pas été volée ou ne pas fait l'objet d'une fraude.

L'opérateur conserve la méthode d'identification utilisée pour identifier l'utilisateur final tant que les données d'identification de celui-ci peuvent être conservées en vertu de l'article 126 de la loi du 13 juin 2005. Les données à conserver par l'opérateur sont déterminées en fonction de la méthode d'identification choisie, mais comprennent au maximum le nom et le prénom, le sexe, la nationalité, la date et le lieu de naissance, l'adresse du domicile, l'adresse e-mail et le numéro de téléphone, le numéro de registre national, le numéro du document d'identité, le pays d'émission du document lorsqu'il s'agit d'un document étranger et la date de validité du document, les références de l'opération de paiement, l'association de la carte prépayée au produit pour lequel l'utilisateur final est déjà identifié et la photo de l'utilisateur final, mais uniquement, en ce qui concerne cette dernière, pour les documents autres que la carte d'identité électronique belge. Lorsque la photo se trouvant sur la carte d'identité électronique belge a été transmise à l'opérateur ou au fournisseur d'un service d'identification, ces derniers détruisent cette photo au plus tard avant l'activation de la carte prépayée.

L'arrêté royal du 27 novembre 2016 définit également les méthodes d'identification valides, à savoir l'identification sur la base de documents d'identification en présence de

l'utilisateur final (article 14), l'identification en ligne et la signature électronique par la carte d'identité électronique auprès de l'entreprise concernée (article 15), l'identification via le fournisseur d'un service d'identification (article 16), l'identification sur la base de l'opération de paiement en ligne (article 17), l'extension ou la migration de produit (article 18) et la vérification par un moyen de communication électronique (article 19).

B.2.6. Lors des travaux préparatoires, la suppression de l'anonymat des cartes de téléphonie mobile prépayées est justifiée comme suit :

« 1) En 2005, le législateur a introduit dans l'article 127, § 3, une dérogation pour les cartes prépayées par rapport à l'interdiction pour un opérateur d'offrir des services qui rendent difficile ou impossible l'identification de l'appelant. Il avait également prévu dans l'article 127, § 1er, une délégation au Roi pour que ce dernier fixe les modalités de l'identification des utilisateurs de cartes prépayées. L'intention du législateur était de mettre fin à l'anonymat pour les cartes prépayées.

2) Le législateur, en ne mettant pas directement fin à l'anonymat pour les cartes prépayées, avait pour but de favoriser la pénétration de la téléphonie mobile. Ce but est entièrement réalisé à l'heure actuelle.

3) La suppression de l'anonymat pour les cartes prépayées est une revendication déjà ancienne des autorités judiciaires (1999), des services de renseignement et de sécurité et des services d'urgence offrant de l'aide sur place. Pour ce qui concerne ces derniers, lors d'un appel d'urgence, ils sont en droit d'obtenir de manière automatique et systématique les données d'identification de l'appelant telles que définies à l'article 2, 57°, de la LCE, dans l'intérêt de la sécurité du citoyen (voir l'article 107 de la LCE).

4) Les cartes prépayées sont très répandues dans les milieux criminels.

5) L'identification de l'utilisateur d'un service de communications électroniques est la première étape à franchir par la Justice ou les services de renseignement ou de sécurité, avant de procéder, le cas échéant, à d'autres mesures. Sans identification, ces autres mesures perdent une grande partie de leur utilité.

6) Actuellement, lorsque la Justice ou les services de renseignement ou de sécurité ne sont pas en mesure d'obtenir l'identification de l'utilisateur final dès lors que cet utilisateur a acheté une carte prépayée de manière anonyme, ils sont amenés à recourir à d'autres techniques pour tout de même identifier la personne recherchée. Ces autres techniques indirectes ont un coût plus important et sont plus intrusives dans la vie privée qu'une simple identification lors de l'achat d'une carte prépayée. Rendre plus efficace l'identification de la personne qui a souscrit à un service en supprimant l'anonymat pour les cartes prépayées a donc pour effet de diminuer les coûts pour la Justice et les services de renseignement et de sécurité (et le nombre de requêtes adressées aux opérateurs) et d'éviter une atteinte inutile à la vie privée de la personne en question et des personnes qui ont des liens avec cette dernière.

7) Comme le relève le Conseil d'État dans son avis n° 58.750/4 du 18 janvier 2016, il convient de relever d'une part, que seuls les acheteurs de cartes prépayées bénéficiaient, à ce jour, de l'anonymat, contrairement aux titulaires d'abonnement, et d'autre part que, dès l'adoption de la LCE, ce régime d'anonymat a été conçu comme destiné à recevoir un caractère temporaire. Dans ce contexte, la disposition à l'examen a donc pour conséquence, en droit et en fait, de rétablir un traitement non différencié entre les utilisateurs des services de communications électroniques concernés, et ainsi, de mettre fin à un traitement différencié temporaire plus favorable aux utilisateurs de cartes prépayées.

Les nouveaux alinéas 2 à 8 de l'article 127, § 1er, sont applicables à l'ensemble des services de communications électroniques. Par contre, le nouvel alinéa 2 introduit dans le paragraphe 3 de l'article 127 est spécifique aux services mobiles fournis sur la base d'une carte prépayée » (*Doc. parl.*, Chambre, 2015-2016, DOC 54-1964/001, pp. 4-6).

B.2.7. Il découle de ce qui précède que l'identifiabilité de tous les utilisateurs finaux de réseaux de communications électroniques constituait dès le départ la prémisse de l'article 127 de la loi du 13 juin 2005 et que l'anonymat des utilisateurs finaux de cartes de téléphonie mobile prépayées a toujours été considéré comme une exception temporaire. En outre, ce n'est pas tant le législateur, mais le Roi qui a supprimé l'anonymat, en prenant l'arrêté royal du 27 novembre 2016.

B.3.1. L'article 16/2 de la loi du 30 novembre 1998, modifié par l'article 3 de la loi attaquée, dispose :

« § 1er. Les services de renseignement et de sécurité peuvent, dans l'intérêt de l'exercice de leurs missions, requérir le concours d'un opérateur de réseaux de communications électroniques ou d'un fournisseur de services de communications électroniques pour procéder à :

1° l'identification de l'abonné ou de l'utilisateur habituel d'un service de communication électronique ou du moyen de communication électronique utilisé;

2° l'identification des services et des moyens de communications électroniques auxquels une personne déterminée est abonnée ou qui sont habituellement utilisés par une personne déterminée.

La réquisition est effectuée par écrit par le dirigeant de service ou son délégué. En cas d'urgence, le dirigeant de service ou son délégué peut requérir ces données verbalement. Cette réquisition verbale est confirmée dans un délai de vingt-quatre heures par une réquisition écrite.

Tout opérateur d'un réseau de communications électroniques et tout fournisseur d'un service de communications électroniques qui est requis donne au dirigeant de service ou à son délégué les données qui ont été demandées dans un délai et selon les modalités à fixer par un

arrêté royal pris sur la proposition du ministre de la Justice, du ministre de la Défense et du ministre qui a les communications électroniques dans ses attributions.

Le dirigeant de service ou son délégué peut, dans le respect des principes de proportionnalité et de subsidiarité, et moyennant l'enregistrement de la consultation, également obtenir les données visées au moyen d'un accès aux fichiers des clients de l'opérateur ou du fournisseur du service. Le Roi fixe, sur la proposition du ministre de la Justice, du ministre de la Défense et du ministre qui a les communications électroniques dans ses attributions, les conditions techniques auxquelles cet accès est possible.

§ 2. Les services de renseignement et de sécurité peuvent, dans l'intérêt de l'exercice de leurs missions, requérir le concours d'une banque ou d'une institution financière pour procéder à l'identification de l'utilisateur final d'une carte prépayée visée dans l'article 127 de la loi du 13 juin 2005 relative aux communications électroniques, sur la base de la référence d'une transaction bancaire électronique qui est liée à la carte prépayée et qui a préalablement été communiquée par un opérateur ou un fournisseur en application du paragraphe 1er.

La réquisition est effectuée par écrit par le dirigeant de service ou son délégué. En cas d'urgence, le dirigeant de service ou son délégué peut requérir ces données verbalement. Cette réquisition verbale est confirmée dans un délai de vingt-quatre heures par une réquisition écrite.

Toute banque et toute institution financière qui est requise donne sans délai au dirigeant de service ou à son délégué les données qui ont été demandées.

Les données d'identification que les services de renseignement et de sécurité reçoivent dans le cadre de l'exercice de la méthode visée au présent paragraphe, se limitent aux données d'identification visées au paragraphe 1er.

§ 3. Toute personne qui refuse de communiquer les données ainsi demandées ou de fournir l'accès requis est punie d'une amende de vingt-six euros à dix mille euros.

§ 4. Les services de renseignement et de sécurité tiennent un registre de toutes les identifications requises et de toutes les identifications obtenues par accès direct. Le Comité permanent R reçoit chaque mois du service de renseignement et de sécurité concerné une liste des identifications requises et de tout accès ».

B.3.2. L'identification sur la base de l'opération de paiement en ligne constitue l'une des méthodes d'identification valides visées dans l'arrêté royal du 27 novembre 2016. L'article 17 de cet arrêté royal dispose :

« § 1er. L'entreprise concernée peut identifier l'utilisateur final sur la base d'une opération de paiement électronique en ligne spécifique à l'achat ou la recharge de la carte prépayée.

Cette méthode est soumise aux conditions suivantes :

1° l'opération de paiement doit être traitée par un prestataire de services de paiement tel que visé à l'art. I.9. 2°, a), b), c), et d) du Code de droit économique;

2° Le prestataire de services de paiement est soumis à la loi du 11 janvier 1993 relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux et du financement du terrorisme;

3° une nouvelle identification doit être effectuée dans les 18 mois qui suivent l'opération de paiement liée à la carte prépayée;

4° l'utilisateur final introduit sur un formulaire en ligne de l'entreprise concernée au minimum son nom, son prénom et le lieu et la date de sa naissance.

§ 2. L'entreprise concernée conserve la référence de l'opération de paiement et les données du formulaire en ligne ».

B.3.3. Lors des travaux préparatoires, le concours que doivent prêter les banques ou les institutions financières a été justifiée comme suit :

« L'arrêté royal relatif à l'identification de l'utilisateur final des services de communications électroniques publics mobiles fournis sur la base d'une carte prépayée déterminera la manière dont un opérateur peut identifier ses utilisateurs finals. Cette identification peut entre autres se faire via une vérification sur la base d'une transaction bancaire en ligne.

Cette dernière méthode d'identification constitue la base de la présente proposition. L'identification via transaction bancaire implique que l'utilisateur final d'une carte prépayée (prepaid) puisse s'identifier sur la base d'une transaction bancaire électronique liée à la carte prépayée. Cette méthode est soumise à plusieurs conditions : (1) la transaction est liée à un compte bancaire dont l'identité du titulaire a préalablement été vérifiée. Cette méthode ne peut pas être appliquée en cas de carte bancaire non traçable, (2) la banque est établie en Belgique. L'opérateur concerné enregistre la référence de la transaction bancaire.

L'identification de l'utilisateur final d'une carte prépayée se fait via l'exercice de deux réquisitions :

1° une réquisition d'un opérateur d'un réseau de communications électroniques, pour l'obtention d'une donnée d'identification (en application de l'actuel article 16/2), à laquelle l'opérateur répond en donnant la référence d'une transaction bancaire, et

2° une réquisition d'une banque ou institution financière pour l'obtention de l'identité de la personne qui se cache derrière cette transaction bancaire (en application du nouveau § 2 de l'article 16/2).

Conformément à la loi du 30 novembre 1998 organique des services de renseignement et de sécurité, la Sûreté de l'État et le Service général du renseignement et de la sécurité des Forces

armées sont habilités à requérir un opérateur d'un réseau de communications électroniques ou un fournisseur d'un service de communications électroniques d'identifier l'abonné ou l'utilisateur habituel d'un service ou moyen de communication électronique.

Cette compétence (classée à l'origine dans la catégorie des ' méthodes spécifiques ') a été requalifiée, par la loi du 5 février 2016 modifiant le droit pénal et la procédure pénale et portant des dispositions diverses en matière de justice (la loi dite pot-pourri II), comme une méthode de renseignement ordinaire. Contrairement aux autres méthodes ordinaires, une série de conditions matérielles et formelles supplémentaires ont toutefois été fixées (compétence uniquement dans le chef du chef de service ou de son délégué et non dans le chef de tout agent de renseignement, enregistrement obligatoire) ainsi qu'un mécanisme de surveillance extérieur supplémentaire (notification mensuelle obligatoire du Comité permanent R qui à son tour en rend compte au Parlement et aux ministres compétents).

La sollicitation auprès d'une banque ou d'une institution financière d'informations sur les transactions bancaires par un service de renseignement et de sécurité (article 18/15 de la loi du 30 novembre 1998) n'est par contre possible que via la procédure définie dans la loi du 30 novembre 1998 d'application pour la catégorie des ' méthodes exceptionnelles '. Cette procédure nécessite un avis conforme préalable de la Commission BIM (la commission chargée de la surveillance des méthodes spécifiques et exceptionnelles de recueil de données par les services de renseignement et de sécurité) et l'autorisation du chef de service. Les méthodes exceptionnelles sont également soumises à des conditions d'application strictes.

Les différentes procédures auxquelles sont soumises les deux réquisitions font en sorte que la méthode d'identification via transaction bancaire (au fond une identification de l'utilisateur d'un service de communications électroniques) devienne dans les faits une méthode exceptionnelle. C'est contraire à l'objectif poursuivi dans la loi Pot-pourri II.

En outre, il convient de garder à l'esprit que pour l'identification de l'utilisateur final d'une carte prépayée, l'information qui est demandée à la banque sert uniquement à retrouver l'identité de celui qui a effectué une transaction bancaire, et par conséquent, ne vise pas à avoir un aperçu de la situation financière de cette personne. Pour obtenir des informations concernant les comptes bancaires, le règlement actuel (méthode exceptionnelle) reste donc d'application. La méthode ordinaire permet de demander en d'autres termes uniquement le nom, le prénom, le sexe, la nationalité, le lieu et la date de naissance, l'adresse et le numéro de registre national de la personne qui est associée au numéro de compte en banque, et ce uniquement dans le cadre de l'identification de l'utilisateur d'une carte SIM prépayée.

Enfin, l'on peut souligner le fait que, dans la présente proposition, l'identification de l'utilisateur final d'une carte prépayée devient il est vrai une méthode ordinaire, mais qu'il y a tout de même des garanties supplémentaires par rapport à d'autres méthodes ordinaires. Ainsi, l'information ne peut pas être sollicitée par n'importe qui, mais seuls le chef de service ou son délégué y sont habilités. De plus, les services de renseignement et de sécurité tiennent un registre de toutes les identifications requises et doivent transmettre chaque mois une liste de ces réquisitions au Comité R » (*Doc. parl.*, Chambre, 2015-2016, DOC 54-1964/001, pp. 14-16).

Quant au premier moyen

B.4. Les parties requérantes prennent un premier moyen de la violation, par l'article 2 de la loi attaquée, des articles 10, 11 et 22 de la Constitution, lus en combinaison avec l'article 8 de la Convention européenne des droits de l'homme, avec les articles 7, 8 et 52 de la Charte des droits fondamentaux de l'Union européenne (ci-après : la Charte) et avec les articles 2, point a), et 6 de la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 « relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données », en ce que cette disposition conférerait au Roi une habilitation trop large et insuffisamment précise pour fixer le contenu de l'obligation d'identification attaquée.

B.5.1. Le principe d'égalité et de non-discrimination n'exclut pas qu'une différence de traitement soit établie entre des catégories de personnes, pour autant qu'elle repose sur un critère objectif et qu'elle soit raisonnablement justifiée.

L'existence d'une telle justification doit s'apprécier en tenant compte du but et des effets de la mesure critiquée ainsi que de la nature des principes en cause; le principe d'égalité et de non-discrimination est violé lorsqu'il est établi qu'il n'existe pas de rapport raisonnable de proportionnalité entre les moyens employés et le but visé.

B.5.2. L'article 22 de la Constitution dispose :

« Chacun a droit au respect de sa vie privée et familiale, sauf dans les cas et conditions fixés par la loi.

La loi, le décret ou la règle visée à l'article 134 garantissent la protection de ce droit ».

L'article 8 de la Convention européenne des droits de l'homme dispose :

« 1. Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance.

2. Il ne peut y avoir ingérence d'une autorité publique dans l'exercice de ce droit que pour autant que cette ingérence est prévue par la loi et qu'elle constitue une mesure qui, dans une

société démocratique, est nécessaire à la sécurité nationale, à la sûreté publique, au bien-être économique du pays, à la défense de l'ordre et à la prévention des infractions pénales, à la protection de la santé ou de la morale, ou à la protection des droits et libertés d'autrui ».

L'article 7 de la Charte dispose :

« Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de ses communications ».

L'article 8 de la Charte dispose :

« 1. Toute personne a droit à la protection des données à caractère personnel la concernant.

2. Ces données doivent être traitées loyalement, à des fins déterminées et sur la base du consentement de la personne concernée ou en vertu d'un autre fondement légitime prévu par la loi. Toute personne a le droit d'accéder aux données collectées la concernant et d'en obtenir la rectification.

3. Le respect de ces règles est soumis au contrôle d'une autorité indépendante ».

L'article 52, paragraphe 1, de la Charte dispose :

« Toute limitation de l'exercice des droits et libertés reconnus par la présente Charte doit être prévue par la loi et respecter le contenu essentiel desdits droits et libertés. Dans le respect du principe de proportionnalité, des limitations ne peuvent être apportées que si elles sont nécessaires et répondent effectivement à des objectifs d'intérêt général reconnus par l'Union ou au besoin de protection des droits et libertés d'autrui ».

L'article 52, paragraphe 3, de la Charte dispose :

« Dans la mesure où la présente Charte contient des droits correspondant à des droits garantis par la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales, leur sens et leur portée sont les mêmes que ceux que leur confère ladite convention. Cette disposition ne fait pas obstacle à ce que le droit de l'Union accorde une protection plus étendue ».

B.5.3. Le Constituant a recherché la plus grande concordance possible entre l'article 22 de la Constitution et l'article 8 de la Convention européenne des droits de l'homme (*Doc. parl.*, Chambre, 1992-1993, n° 997/5, p. 2).

La portée de cet article 8 est analogue à celle de la disposition constitutionnelle précitée, de sorte que les garanties que fournissent ces deux dispositions forment un tout indissociable.

Lorsque la Charte contient des droits correspondant à des droits garantis par la Convention européenne des droits de l'homme, « leur sens et leur portée sont les mêmes que ceux que leur confère ladite convention ». Cette disposition aligne le sens et la portée des droits qui sont garantis par la Charte sur les droits correspondants qui sont garantis par la Convention européenne des droits de l'homme.

Les explications relatives à la Charte (2007/C 303/02), publiées au *Journal officiel* du 14 décembre 2007, indiquent que, parmi les articles « dont le sens et la portée sont les mêmes que ceux des articles correspondants dans la CEDH », l'article 7 de la Charte correspond à l'article 8 de la Convention européenne des droits de l'homme.

La Cour de justice de l'Union européenne rappelle à cet égard que « l'article 7 de la Charte, relatif au droit au respect de la vie privée et familiale, contient des droits correspondant à ceux garantis par l'article 8, paragraphe 1, de la [Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales, signée à Rome le 4 novembre 1950 (ci-après : la CEDH),] et qu'il convient donc, conformément à l'article 52, paragraphe 3, de la Charte, de donner audit article 7 le même sens et la même portée que ceux conférés à l'article 8, paragraphe 1, de la CEDH, tel qu'interprété par la jurisprudence de la Cour européenne des droits de l'homme » (CJUE, 17 décembre 2015, C-419/14, *WebMindLicenses Kft.*, point 70; 14 février 2019, C-345/17, *Buivids*, point 65).

En ce qui concerne l'article 8 de la Charte, la Cour de justice considère qu'« ainsi que le prévoit expressément l'article 52, paragraphe 3, seconde phrase, de la Charte, l'article 52, paragraphe 3, première phrase, de celle-ci ne fait pas obstacle à ce que le droit de l'Union accorde une protection plus étendue que la CEDH », et que « l'article 8 de la Charte concerne un droit fondamental distinct de celui consacré à l'article 7 de celle-ci et qui n'a pas d'équivalent dans la CEDH » (CJUE, grande chambre, 21 décembre 2016, C-203/15 et C-698/15, *Tele2 Sverige*, point 129).

Il découle de ce qui précède que, dans le champ d'application du droit de l'Union européenne, l'article 22 de la Constitution, l'article 8 de la Convention européenne des droits de l'homme et l'article 7 de la Charte garantissent des droits fondamentaux analogues, alors que l'article 8 de cette Charte vise spécifiquement la protection des données à caractère personnel.

B.5.4. En vertu de l'article 94, paragraphe 1, du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 « relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) » (ci-après : le RGPD), la directive 95/46/CE est abrogée avec effet au 25 mai 2018.

L'article 5 du RGPD, qui a reproduit *mutatis mutandis* le contenu de l'article 6 de la directive 95/46/CE, dispose :

« 1. Les données à caractère personnel doivent être :

a) traitées de manière licite, loyale et transparente au regard de la personne concernée (licéité, loyauté, transparence);

b) collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement d'une manière incompatible avec ces finalités; le traitement ultérieur à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques n'est pas considéré, conformément à l'article 89, paragraphe 1, comme incompatible avec les finalités initiales (limitation des finalités);

c) adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées (minimisation des données);

d) exactes et, si nécessaire, tenues à jour; toutes les mesures raisonnables doivent être prises pour que les données à caractère personnel qui sont inexactes, eu égard aux finalités pour lesquelles elles sont traitées, soient effacées ou rectifiées sans tarder (exactitude);

e) conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées; les données à caractère personnel peuvent être conservées pour des durées plus longues dans la mesure où elles seront traitées exclusivement à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques conformément à l'article 89, paragraphe 1, pour autant que soient mises en œuvre les mesures techniques et organisationnelles appropriées requises par le présent règlement afin de garantir les droits et libertés de la personne concernée (limitation de la conservation);

f) traitées de façon à garantir une sécurité appropriée des données à caractère personnel, y compris la protection contre le traitement non autorisé ou illicite et contre la perte, la destruction ou les dégâts d'origine accidentelle, à l'aide de mesures techniques ou organisationnelles appropriées (intégrité et confidentialité).

2. Le responsable du traitement est responsable du respect du paragraphe 1 et est en mesure de démontrer que celui-ci est respecté (responsabilité) ».

B.6. En réservant au législateur compétent le pouvoir de fixer dans quels cas et à quelles conditions il peut être porté atteinte au droit au respect de la vie privée, l'article 22 de la Constitution garantit à tout justiciable qu'aucune ingérence dans l'exercice de ce droit ne peut avoir lieu qu'en vertu de règles adoptées par une assemblée délibérante, démocratiquement élue.

Une délégation au pouvoir exécutif n'est toutefois pas contraire au principe de la légalité, pour autant que l'habilitation soit définie de manière suffisamment précise et qu'elle porte sur l'exécution de mesures dont les éléments essentiels ont été fixés préalablement par le législateur.

B.7.1. Selon le Conseil des ministres, le moyen est irrecevable, étant donné que la disposition attaquée comporte seulement une nouvelle délégation au Roi, plus précisément la délégation qui a été insérée dans le nouvel article 127, § 3, alinéa 2, de la loi du 13 juin 2005 et qui n'est pas attaquée par les parties requérantes. Les autres délégations au Roi étaient déjà contenues dans l'article 127 de cette loi avant l'entrée en vigueur de la disposition attaquée.

B.7.2. Un recours dirigé contre une différence de traitement ne résultant pas de la loi attaquée mais déjà contenue dans une loi antérieure est irrecevable.

Toutefois, lorsque, dans une législation nouvelle, le législateur reprend une disposition ancienne et s'approprie de cette manière son contenu, un recours peut être introduit contre la disposition reprise, dans les six mois de sa publication.

B.7.3. La disposition attaquée a modifié l'article 127 de la loi du 13 juin 2005 sur différents points, même si, à cette occasion, comme il est dit en B.2.7, le législateur est resté fidèle à la prémisse initiale de l'identifiabilité de tous les utilisateurs finaux de réseaux de

communications électroniques. En édictant la disposition attaquée, il s'est donc approprié le contenu de l'article 127 de la loi du 13 juin 2005.

L'exception est rejetée.

B.8.1. La Commission de la protection de la vie privée (actuellement l'Autorité de protection des données) a formulé, dans un avis relatif à l'avant-projet ayant donné lieu à la loi attaquée, quelques observations concernant le respect du principe de la légalité en matière de restrictions du droit au respect de la vie privée :

« 10. L'avant-projet de loi règle spécifiquement cette question, ce qui permet de répondre à la condition de forme susmentionnée d'une base légale. La Commission constate cependant que le législateur a omis d'intégrer plusieurs éléments essentiels dans le texte légal. L'avant-projet de loi et l'Exposé des motifs renvoient tous les deux aux mesures d'exécution à prendre concernant les spécifications du traitement de données envisagé, qui seront définies par arrêté royal, à savoir la désignation du responsable du traitement, l'indication de qui a accès aux données, la définition du délai de conservation, …. En l'absence de textes concrets, la Commission n'est actuellement pas en mesure d'émettre un avis sur les mesures d'exécution envisagées. La Commission souligne qu'une fois disponibles, les futurs arrêtés d'exécution (portant exécution de l'article 127 de la loi télécom) devront lui être préalablement soumis pour avis afin de pouvoir les confronter aux exigences de la loi vie privée, notamment en matière de proportionnalité. Il est recommandé d'intégrer cette demande d'avis préalable concernant les arrêtés d'exécution dans le texte législatif proprement dit.

[…]

14. Comme mentionné ci-avant […], la Commission recommande de préciser dans le texte législatif que l'identification des cartes prépayées achetées avant le 1er mai 2016 s'effectuera également au moyen des données d'identification devant être conservées en vertu de l'article 126. Il ne serait pas logique de prévoir d'autres catégories de données pour les utilisateurs existants. La nature des données doit être déterminée par la loi. L'arrêté d'exécution porte uniquement sur les mesures d'exécution et la date de mise en œuvre.

15. L'Exposé des motifs de l'avant-projet de loi explique en outre l'intention de compléter les données d'identification devant être conservées en vertu de l'article 126 avec le numéro de Registre national. Il est essentiel de reprendre cette explication telle quelle dans le texte législatif proprement dit.

[…]

PAR CES MOTIFS,

la Commission,

émet un avis favorable concernant l'avant-projet de loi modifiant la loi du 13 juin 2005 relative aux communications électroniques à la condition stricte qu'il soit tenu compte de ses remarques, et plus particulièrement celles visant :

- à lui soumettre pour avis les arrêtés d'exécution planifiés en vue notamment du contrôle de la proportionnalité (points 10 et 20);

- à mentionner explicitement dans la loi relative aux communications électroniques l'utilisation du numéro de Registre national, exclusivement en ce qui concerne les cartes prépayées (point 17);

- à préciser l'avant-projet de loi la nature des données, à savoir les données d'identification devant être conservées en vertu de l'article 126, complétées par le numéro de Registre national, et ce aussi bien pour les cartes achetées le 1er mai 2016 et après cette date, que pour les cartes achetées avant cette date (points 14-15) » (CPVP, avis n° 54/2015, 15 décembre 2015, *Doc. parl.*, Chambre, 2015-2016, DOC 54-1964/001, pp. 38-42).

La section de législation du Conseil d'État a elle aussi formulé, dans son avis relatif à cet avant-projet, quelques observations sur le respect du principe de la légalité en matière de restrictions du droit au respect de la vie privée :

« 1.2.4. Les habilitations consenties au Roi par l'article 127, § 1er, alinéas 6 et 7 en projet sont excessivement larges : c'est au législateur qu'il appartient de déterminer les cas dans lesquels l'opérateur pourra ou devra faire une copie du document permettant d'établir l'identité de l'utilisateur final, de même que c'est à lui qu'il appartient de déterminer quel est ce document.

Par ailleurs, il convient que le législateur fixe les critères à mettre en œuvre par le Roi pour établir des méthodes d'identification différenciées, assorties de dates d'entrée en vigueur différenciées, selon que les cartes prépayées sont activées avant ou après une date fixée par le Roi. À cet égard, les explications figurant dans le commentaire de l'article gagneraient à être, pour l'essentiel, intégrées dans le dispositif en projet lui-même, sous la forme de critères à mettre en œuvre par le Roi, et pour le surplus, à être étoffées, dans le commentaire de l'article.

1.2.5. Si l'auteur de l'avant-projet a l'intention d'imposer la conservation non seulement des données d'identification – par définition, pendant le délai prévu à l'article 126 de la loi du 13 juin 2005 – mais également des documents ayant permis de recueillir ces données, c'est au législateur lui-même qu'il appartient d'imposer cette obligation et d'en déterminer le délai - lequel ne saurait évidemment être supérieur à celui prévu par l'article 126 » (Conseil d'État, section de législation, avis n° 59.423/4, 15 juin 2016, *Doc. parl.*, Chambre, 2015-2016, DOC 54-1964/001, pp. 47-48).

B.8.2. Le législateur n'a que partiellement suivi ces avis. Il a notamment choisi, en dépit de ceux-ci, de ne pas indiquer dans la disposition attaquée les données d'identification qui peuvent être collectées et traitées et les documents d'identification qui entrent en considération. Ce choix a été justifié lors des travaux préparatoires comme suit :

« Premièrement, à l'exception de l'utilisation du numéro de registre national, c'est l'arrêté royal d'exécution de l'article 127, § 1er, alinéa 1er, de la loi (le projet d'arrêté royal ' cartes prépayées ') et non cet article qui définit les données d'identification à collecter.

En effet, les données d'identification précises à collecter, à l'exception du numéro de registre national, ne sont pas les éléments essentiels de la matière. D'ailleurs, la Commission de la protection de la vie privée, dans son premier avis sur le projet de loi (avis n° 54/2015 du 16 décembre 2015), ne demande pas que la liste des données à collecter soit reprise dans la loi mais uniquement d'indiquer ' la nature des données, à savoir les données d'identification devant être conservées en vertu de l'article 126 '. Pour répondre à la demande de la Commission vie privée, le projet de loi prévoit que les données d'identification collectées sont conservées conformément à l'article 126, § 3, alinéa 1er, de la loi.

De plus, pour la conservation des données, c'est l'arrêté royal du 19 septembre 2013 portant exécution de l'article 126 de la loi du 13 juin 2005 relative aux communications électroniques et non l'article 126 qui fixe les données à conserver. Par analogie, c'est le projet d'arrêté royal ' cartes prépayées ' qui comprend les données d'identification à collecter et non l'article 127 de la loi, qui est la base légale de cet arrêté royal. Tant l'article 127 que l'article 126 constituent des restrictions aux libertés fondamentales.

Finalement, il n'est pas adéquat que la liste exacte des données d'identification à collecter soit reprise dans la loi, vu le caractère technique de ces données, le fait que ces données sont intimement liées aux méthodes d'identification développées dans l'arrêté royal ' cartes prépayées ' en projet (et ne peuvent être comprises qu'en lisant cet arrêté royal) et la nécessité éventuelle de les adapter à l'avenir en fonction des enseignements de la pratique ou des évolutions futures.

Deuxièmement, c'est le projet d'arrêté royal ' cartes prépayées ' et non l'article 127 de la loi qui déterminera la liste complète des documents d'identification qui sont acceptés.

En effet, il ne s'agit pas d'un élément essentiel de la législation (l'élément essentiel est par contre que l'identification doit se faire sur base d'un document d'identification valide).

Par ailleurs, reprendre cette liste dans la loi l'alourdirait (vu les nombreux documents d'identification qui devraient être admis) et aurait comme inconvénient de ne pas pouvoir facilement l'adapter en fonction des enseignements tirés de la pratique et des évolutions.

Troisièmement, le projet de loi ne développe pas de critères pour encadrer la délégation au Roi concernant la différenciation entre les nouvelles et les anciennes cartes prépayées comme demandé par le Conseil d'Etat. En effet, les méthodes d'identification pour les anciennes et les nouvelles cartes prépayées sont en réalité les mêmes : un utilisateur final d'une nouvelle carte

prépayée et un utilisateur final d'une ancienne carte prépayée qui n'a pas encore été identifié doivent s'identifier selon les mêmes méthodes d'identification.

Par contre, le projet de loi fixe directement les règles applicables (voir le nouvel alinéa introduit au paragraphe 3 de l'article 127). La délégation au Roi ne portera plus que sur la définition de ce qu'est un utilisateur final d'une carte ancienne qui a déjà été identifié.

Par sa lettre du 1er juillet 2016 au Vice-Premier ministre et ministre des Télécommunications […], la Commission de la protection de la vie privée a indiqué ne pas avoir de commentaire sur ce projet » (*Doc. parl.*, Chambre, 2015-2016, DOC 54-1964/001, pp. 6-7).

B.8.3.1. L'article 127 de la loi du 13 juin 2005 règle lui-même le principe de l'identifiabilité de l'utilisateur final tant des anciennes cartes prépayées que des nouvelles. Il lie la suppression de l'anonymat des cartes prépayées à la date à laquelle l'arrêté d'exécution entre en vigueur et y ajoute qu'il est interdit, à partir de cette date, de fournir des services ou des équipements susceptibles de rendre l'identification difficile. Il dispose aussi que, sauf preuve contraire, l'utilisateur final identifié est présumé utiliser lui-même le service de communications électroniques.

Il mentionne également les catégories de personnes à qui sont imposées des obligations dans ce contexte, à savoir les opérateurs, les fournisseurs, les canaux de vente, les entreprises qui fournissent un service d'identification et les utilisateurs finaux. Il définit enfin le but de l'identifiabilité, à savoir le bon fonctionnement des services d'urgence, l'enquête pénale et le fonctionnement des services de renseignement et de sécurité.

B.8.3.2. Sur le plan de l'identifiabilité, l'article 127 de la loi du 13 juin 2005 confère plusieurs habilitations au Roi. Tout d'abord, il L'habilite à fixer, de manière générale, les mesures techniques et administratives qui doivent être imposées dans ce contexte aux parties concernées. Il doit également déterminer qui sont les utilisateurs finaux non identifiés de cartes prépayées achetées avant l'entrée en vigueur de l'arrêté d'exécution. Il doit aussi fixer le délai maximal dans lequel les utilisateurs finaux non identifiés doivent s'identifier auprès de leur opérateur, même si l'article 127 de la loi du 13 juin 2005 limite cette habilitation en disposant que ce délai ne peut pas excéder six mois. Enfin, le Roi doit déterminer les tarifs rétribuant le concours des opérateurs et des fournisseurs à l'identification d'un utilisateur final.

Ces habilitations portent sur l'exécution de mesures dont les éléments essentiels ont été préalablement déterminés par le législateur.

B.8.4.1. Pour ce qui est des données d'identification et des documents d'identification concernés, l'article 127 de la loi attaquée dispose qu'il doit s'agir de documents comportant le numéro de registre national et que le numéro de registre national est une donnée à caractère personnel qui doit être collectée et traitée dans ce contexte. Les autres données d'identification, ainsi que les documents d'identification qui entrent en considération, ne sont pas énumérés dans cette disposition législative, en dépit des avis mentionnés en B.8.1.

B.8.4.2. En outre, le législateur n'a pas donné au Roi une habilitation explicite pour définir plus précisément ces données d'identification et ces documents d'identification. De tels éléments essentiels d'un traitement de données à caractère personnel ne sauraient toutefois être couverts par l'habilitation vague conférée par l'article 127, § 1er, alinéa 1er, de la loi du 13 juin 2005 et qui consiste à prendre les « mesures techniques et administratives » nécessaires en vue de l'identifiabilité de l'utilisateur final.

Le Roi devait dès lors déterminer ces données et ces documents d'identification sur la base du pouvoir qu'Il tire de l'article 108 de la Constitution de faire les règlements et les arrêtés nécessaires pour l'exécution des lois.

Toutefois, ce pouvoir général d'exécution du Roi ne saurait suffire en l'espèce. En effet, la délégation d'éléments essentiels d'une matière réservée par le Constituant au pouvoir législatif n'est possible que si le respect de la procédure parlementaire ne permet pas au législateur de réaliser un objectif d'intérêt général et à condition qu'il détermine explicitement et sans équivoque l'objet de cette habilitation et que les mesures prises par le Roi soient examinées par le pouvoir législatif, en vue de leur confirmation, dans un délai relativement court, fixé dans la loi d'habilitation.

B.8.4.3. Lors des travaux préparatoires, le législateur justifie cette méthode de travail par le caractère technique des données d'identification et des documents d'identification, la nécessité de pouvoir en adapter l'énumération en fonction de nouveaux enseignements et le fait que, dans le cadre de la conservation des données, ces données n'étaient pas non plus énumérées

dans l'article 126 de la loi du 13 juin 2005 lui-même annulé par l'arrêt de la Cour n° 57/2021 du 22 avril 2021.

Indépendamment du fait que ces arguments ne sauraient expliquer l'absence d'une habilitation explicite et sans équivoque, le caractère technique des données d'identification et des documents d'identification et l'adaptabilité d'une telle énumération ne suffisent pas pour conclure que le fait d'ancrer de tels éléments dans une norme législative ne permettrait pas au législateur de réaliser un objectif d'intérêt général. En effet, même une norme législative peut être modifiée. Le Conseil des ministres ne démontre pas qu'une modification de ces données d'identification peut être urgente au point de ne pas pouvoir suivre le cours normal de la procédure législative. De même, une énumération des données d'identification et des documents d'identification n'est pas complexe au point de ne pas pouvoir être inscrite dans une norme législative. Enfin, le législateur ne saurait justifier une violation de la Constitution en renvoyant à une autre disposition législative qui comportait peut-être la même inconstitutionnalité.

B.8.4.4. Au demeurant, l'article 127 de la loi du 13 juin 2005 délimite insuffisamment le pouvoir d'exécution du Roi pour déterminer les données d'identification qui sont collectées et traitées et les documents d'identification qui entrent en considération. En ce qui concerne les documents d'identification, il mentionne seulement qu'il doit s'agir de documents comprenant le numéro de registre national. En ce qui concerne les données d'identification autres que le numéro de registre national, il ne comporte pas la moindre précision.

B.8.5. Pour ce qui est de la collecte et du traitement des données et des documents d'identification, l'article 127 de la loi du 13 juin 2005 définit qui collecte les données, à savoir le canal de vente ou l'entreprise qui offre un service d'identification. Il dispose également que le canal de vente ne peut pas conserver ces données et ces documents et qu'il doit les détruire au plus tard au moment de l'activation de la carte de téléphonie mobile prépayée.

En ce qui concerne le mode de traitement des données, l'article 127 de la loi du 13 juin 2005 définit qui est le responsable du traitement, à savoir l'opérateur ou le fournisseur. Il dispose également que le canal de vente transmet les données collectées à l'opérateur, au fournisseur ou à l'entreprise qui offre un service d'identification, par une introduction directe dans un système informatique ou à l'aide d'une copie du document d'identification. Il dispose

également que l'opérateur et le fournisseur doivent conserver une copie de tout document d'identification autre que la carte d'identité électronique belge et que les données d'identification traitées doivent être conservées conformément à l'article 126, § 3, de la loi du 13 juin 2005.

B.8.6. En ce qui concerne les sanctions, l'article 127, §§ 4 et 5, de la loi du 13 juin 2005 dispose que les opérateurs ou les fournisseurs qui ne respectent pas les mesures techniques et administratives imposées par le Roi ne peuvent plus fournir le service pour lequel ces mesures n'ont pas été prises. Il dispose également que les utilisateurs finaux qui ne respectent pas les obligations qui leur incombent doivent être déconnectés, sans indemnité, du réseau de communications électroniques.

B.8.7.1. Les parties requérantes reprochent en outre à la disposition attaquée de ne pas fixer des critères distincts pour les utilisateurs finaux d'anciennes et de nouvelles cartes prépayées.

L'article 127 de la loi du 13 juin 2005, tel qu'il a été modifié par l'article 2 de la loi attaquée, soumet toutefois les deux catégories d'utilisateurs finaux de manière égale à l'obligation d'identifiabilité. À cet égard, l'article 127, § 3, alinéa 2, de cette loi fixe un délai maximal dans lequel les utilisateurs finaux d'anciennes cartes prépayées doivent satisfaire aux mesures administratives et techniques fixées par le Roi, alors que la nouvelle réglementation était applicable aux nouvelles cartes prépayées dès son entrée en vigueur.

B.8.7.2. En ce que les parties requérantes reprochent à la disposition attaquée de ne pas préciser suffisamment clairement les catégories d'utilisateurs finaux de réseaux de communications électroniques auxquelles elle s'applique, il suffit de constater que, conformément à l'objectif initial de l'article 127 de la loi du 13 juin 2005, tous les utilisateurs finaux relèvent de son champ d'application, indépendamment du fait qu'ils disposent d'un abonnement ou d'une carte de téléphonie mobile prépayée. Comme il est dit en B.2.6, l'assimilation des utilisateurs finaux d'une carte de téléphonie mobile prépayée aux titulaires d'abonnements constitue d'ailleurs l'un des objectifs de la loi attaquée.

B.8.7.3. En ce que les parties requérantes reprochent à la disposition attaquée de ne pas préciser les circonstances du traitement des données, il y a lieu de constater que cette disposition renvoie à cet égard à l'article 126, § 3, de la loi du 13 juin 2005.

Par son arrêt n° 57/2021 du 22 avril 2021, la Cour a annulé notamment l'article 4 de la loi du 29 mai 2016 « relative à la collecte et à la conservation des données dans le secteur des communications électroniques ». Par son arrêt n° 84/2015 du 11 juin 2015, la Cour avait déjà annulé la loi du 30 juillet 2013 « portant modification des articles 2, 126 et 145 de la loi du 13 juin 2005 relative aux communications électroniques et de l'article 90*decies* du Code d'instruction criminelle ». À la suite de ces arrêts, l'article 126 de la loi du 13 juin 2005 est actuellement applicable dans la version qui a été modifiée pour la dernière fois par l'article 33 de la loi du 4 février 2010 « relative aux méthodes de recueil des données par les services de renseignement et de sécurité ». Les annulations mentionnées reposaient en substance sur l'interdiction d'une conservation généralisée et indifférenciée des données. Cette interdiction trouvant son fondement dans le droit de l'Union, l'article 126 de la loi du 13 juin 2005 ne saurait être réputé applicable dans la version qui précède ces annulations, en ce que celle-ci porte sur une conservation généralisée et indifférenciée des données en matière de communications électroniques. La même disposition peut cependant être applicable en ce qu'elle porte sur les données d'identification des utilisateurs de cartes de téléphonie mobile prépayées visées à l'article 127 de la même loi. L'article 126, tel qu'il a été modifié par la loi du 4 février 2010, dispose :

« § 1er. Par arrêté délibéré en Conseil des Ministres, le Roi fixe, sur proposition du Ministre de la Justice et du ministre et après avis de la Commission pour la protection de la vie privée et de l'Institut, les conditions dans lesquelles les opérateurs enregistrent et conservent les données de trafic et les données d'identification d'utilisateurs finals en vue de la poursuite et la répression d'infractions pénales, en vue de la répression d'appels malveillants vers les services d'urgence et en vue de la recherche par le service de médiation pour les télécommunications de l'identité des personnes ayant effectué une utilisation malveillante d'un réseau ou d'un service de communications électroniques, ainsi qu'en vue de l'accomplissement des missions de renseignement prévues par la loi du 30 novembre 1998 organique des services de renseignement et de sécurité.

§ 2. Les données à conserver ainsi que la durée de la conservation, qui en matière de service téléphonique accessible au public ne peut ni être inférieure à douze mois ni dépasser trente-six mois, sont déterminées par le Roi dans un arrêté délibéré en Conseil des ministres, après avis de la Commission pour la protection de la vie privée et de l'Institut.

Les opérateurs font en sorte que les données reprises au § 1er soient accessibles de manière illimitée de Belgique ».

En exécution de cette disposition, l'arrêté royal du 19 septembre 2013 « portant exécution de l'article 126 de la loi du 13 juin 2005 relative aux communications électroniques » (ci-après : l'arrêté royal du 19 septembre 2013) règle actuellement le traitement et la conservation des données à caractère personnel, y compris en ce qui concerne les données d'identification qui sont collectées sur la base de l'article 127 de la loi du 13 juin 2005.

Dans son mémoire complémentaire et lors de l'audience, le Conseil des ministres a d'ailleurs souligné qu'une nouvelle version de l'article 126 de la loi du 13 juin 2005 est en préparation, pour satisfaire aux exigences de l'arrêt de la Cour n° 57/2021 et de la jurisprudence de la Cour de justice de l'Union européenne qui y est appliquée.

B.8.7.4. En ce que les parties requérantes reprochent à la disposition attaquée de ne pas déterminer qui a accès aux données d'identification conservées ni les conditions de cet accès, il suffit de constater que cet accès n'est pas réglé par l'article 127 de la loi du 13 juin 2005, mais par les articles 46*bis*, 88*bis* et 90*ter* à 90*decies* du Code d'instruction criminelle en ce qui concerne l'accès dans le cadre d'une instruction pénale, par l'article 16/2, § 1er, de la loi du 30 novembre 1998 en ce qui concerne l'accès par les services de renseignement et de sécurité et par l'article 107, § 2, de la loi du 13 juin 2005 en ce qui concerne l'accès par les services d'urgence.

B.8.8. En outre, en accordant une telle délégation, le législateur ne pouvait habiliter le Roi à prendre des dispositions qui entraîneraient une violation du droit au respect de la vie privée. Il appartient au juge compétent de vérifier si le Roi a fait un usage légal ou non de la délégation qui Lui est accordée.

B.9.1. Il ressort de ce qui précède que l'article 127 de la loi du 13 juin 2005, tel qu'il a été modifié par l'article 2 de la loi attaquée, viole le principe de légalité garanti par l'article 22 de la Constitution, mais seulement en ce qu'il ne détermine pas les données d'identification qui sont collectées et traitées et les documents d'identification qui entrent en considération. Dans cette mesure, il y a lieu d'annuler l'article 2 de la loi attaquée.

Pour le surplus, le premier moyen n'est pas fondé, étant donné que les habilitations conférées au Roi et qui sont attaquées portent sur l'exécution de mesures dont les éléments essentiels ont été fixés au préalable par le législateur.

B.9.2. Contrairement à ce que les parties requérantes font valoir, la Cour européenne des droits de l'homme n'a pas jugé, par son arrêt *Rotaru*, que le traitement des données à caractère personnel et l'accès aux données traitées doivent être réglés par le pouvoir législatif. Elle a seulement souligné que ce traitement et cet accès doivent avoir une base claire, accessible et prévisible dans la réglementation interne (CEDH, grande chambre, 4 mai 2000, *Rotaru c. Roumanie*, §§ 47-63).

La Cour de justice aussi exige seulement que « la base légale qui permet l'ingérence dans [le droit au respect de la vie privée] doit définir elle-même la portée de la limitation de l'exercice du droit concerné » (CJUE, 6 octobre 2020, C-623/17, *Privacy international*, point 65). Elle n'exige pas que tous les aspects de cette limitation soient réglés par une loi formelle.

Un contrôle de la disposition attaquée au regard de l'article 8 de la Convention européenne des droits de l'homme, des articles 7 et 8 de la Charte ou de l'article 5 du RGPD ne conduit dès lors pas à une autre conclusion, étant donné que ces dispositions ne permettent pas de déduire des exigences plus strictes en ce qui concerne le principe de la légalité formelle que celles qui découlent de l'article 22 de la Constitution.

B.9.3. Étant donné que la violation constatée porte uniquement sur l'article 22 de la Constitution et non sur les normes du droit de l'Union européenne invoquées dans le moyen, il appartient à la Cour, en vertu de l'article 8, alinéa 3, de la loi spéciale du 6 janvier 1989 sur la Cour constitutionnelle, d'indiquer ceux des effets des dispositions annulées qui doivent être considérés comme définitifs ou maintenus provisoirement pour le délai qu'elle détermine.

La violation constatée de l'article 22 de la Constitution ne porte pas sur la nature et le contenu des données d'identification ou des documents d'identification tels qu'ils sont actuellement réglés dans l'arrêté royal du 27 novembre 2016 et tels qu'ils échappent au pouvoir de contrôle de la Cour. Elle porte uniquement sur le fait que ces données et documents doivent être énumérés dans une disposition législative.

Il y a donc lieu de donner au législateur le temps nécessaire pour prévoir ce fondement légal, sans qu'il faille dans l'intervalle annuler l'identification des utilisateurs finaux de cartes de téléphonie mobile prépayées réglée par la disposition attaquée. En outre, ce délai doit être suffisamment long pour permettre au législateur d'aligner ce fondement légal sur la nouvelle réglementation en matière de conservation des données qui est en préparation, à la suite de l'arrêt de la Cour n° 57/2021 du 22 avril 2021.

Par conséquent, il y a lieu de maintenir les effets de la disposition attaquée comme il est indiqué dans le dispositif.

Quant au deuxième moyen

B.10. Les parties requérantes prennent un deuxième moyen de la violation, par les articles 2 et 3 de la loi attaquée, des articles 10, 11, 19, 22 et 25 de la Constitution, lus en combinaison avec les articles 8 et 10 de la Convention européenne des droits de l'homme, avec les articles 7, 8, 11 et 52 de la Charte, avec les articles 56 et 57 du Traité sur le fonctionnement de l'Union européenne, avec les articles 2, point a), et 6 de la directive 95/46/CE et avec les articles 1er, 2, 3, 5, 6, 9 et 15 de la directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 « concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques) ». Ce moyen se subdivise en trois branches.

B.11.1. L'article 19 de la Constitution dispose :

« La liberté des cultes, celle de leur exercice public, ainsi que la liberté de manifester ses opinions en toute matière, sont garanties, sauf la répression des délits commis à l'occasion de l'usage de ces libertés ».

L'article 25 de la Constitution dispose :

« La presse est libre; la censure ne pourra jamais être établie; il ne peut être exigé de cautionnement des écrivains, éditeurs ou imprimeurs.

Lorsque l'auteur est connu et domicilié en Belgique, l'éditeur, l'imprimeur ou le distributeur ne peut être poursuivi ».

L'article 10 de la Convention européenne des droits de l'homme dispose :

« 1. Toute personne a droit à la liberté d'expression. Ce droit comprend la liberté d'opinion et la liberté de recevoir ou de communiquer des informations ou des idées sans qu'il puisse y avoir ingérence d'autorités publiques et sans considération de frontière. Le présent article n'empêche pas les États de soumettre les entreprises de radiodiffusion, de cinéma ou de télévision à un régime d'autorisations.

2. L'exercice de ces libertés comportant des devoirs et des responsabilités peut être soumis à certaines formalités, conditions, restrictions ou sanctions prévues par la loi, qui constituent des mesures nécessaires, dans une société démocratique, à la sécurité nationale, à l'intégrité territoriale ou à la sûreté publique, à la défense de l'ordre et à la prévention du crime, à la protection de la santé ou de la morale, à la protection de la réputation ou des droits d'autrui, pour empêcher la divulgation d'informations confidentielles ou pour garantir l'autorité et l'impartialité du pouvoir judiciaire ».

L'article 11 de la Charte dispose :

« 1. Toute personne a droit à la liberté d'expression. Ce droit comprend la liberté d'opinion et la liberté de recevoir ou de communiquer des informations ou des idées sans qu'il puisse y avoir ingérence d'autorités publiques et sans considération de frontières.

2. La liberté des médias et leur pluralisme sont respectés ».

En ce qu'ils reconnaissent le droit à la liberté d'expression, l'article 10 de la Convention européenne des droits de l'homme et l'article 11, paragraphe 1, de la Charte ont une portée analogue à celle de l'article 19 de la Constitution, qui reconnaît la liberté de manifester ses opinions en toute matière.

Dès lors, les garanties fournies par ces dispositions forment, dans cette mesure, un ensemble indissociable.

B.11.2. L'article 56 du Traité sur le fonctionnement de l'Union européenne dispose :

« Dans le cadre des dispositions ci-après, les restrictions à la libre prestation des services à l'intérieur de l'Union sont interdites à l'égard des ressortissants des États membres établis dans un État membre autre que celui du destinataire de la prestation.

Le Parlement européen et le Conseil, statuant conformément à la procédure législative ordinaire, peuvent étendre le bénéfice des dispositions du présent chapitre aux prestataires de services ressortissants d'un État tiers et établis à l'intérieur de l'Union ».

L'article 57 du Traité sur le fonctionnement de l'Union européenne dispose :

« Au sens des traités, sont considérées comme services les prestations fournies normalement contre rémunération, dans la mesure où elles ne sont pas régies par les dispositions relatives à la libre circulation des marchandises, des capitaux et des personnes.

Les services comprennent notamment :

a) des activités de caractère industriel,

b) des activités de caractère commercial,

c) des activités artisanales,

d) les activités des professions libérales.

Sans préjudice des dispositions du chapitre relatif au droit d'établissement, le prestataire peut, pour l'exécution de sa prestation, exercer, à titre temporaire, son activité dans l'État membre où la prestation est fournie, dans les mêmes conditions que celles que cet État impose à ses propres ressortissants ».

B.11.3. Les articles 1er, 2, 3, 5, 6, 9 et 15 de la directive 2002/58/CE disposent :

« Article premier. Champ d'application et objectif

1. La présente directive prévoit l'harmonisation des dispositions nationales nécessaires pour assurer un niveau équivalent de protection des droits et libertés fondamentaux, et en particulier du droit à la vie privée, en ce qui concerne le traitement des données à caractère personnel dans le secteur des communications électroniques, ainsi que la libre circulation de ces données et des équipements et des services de communications électroniques dans la Communauté.

2. Les dispositions de la présente directive précisent et complètent la directive 95/46/CE aux fins énoncées au paragraphe 1. En outre, elles prévoient la protection des intérêts légitimes des abonnés qui sont des personnes morales.

3. La présente directive ne s'applique pas aux activités qui ne relèvent pas du traité instituant la Communauté européenne, telles que celles visées dans les titres V et VI du traité sur l'Union européenne, et, en tout état de cause, aux activités concernant la sécurité publique, la défense, la sûreté de l'État (y compris la prospérité économique de l'État lorsqu'il s'agit d'activités liées à la sûreté de l'État) ou aux activités de l'État dans des domaines relevant du droit pénal.

Article 2. Définitions

Sauf disposition contraire, les définitions figurant dans la directive 95/46/CE et dans la directive 2002/21/CE du Parlement européen et du Conseil du 7 mars 2002 relative à un cadre réglementaire commun pour les réseaux et les services de communications électroniques (directive ‘ cadre ’) s’appliquent aux fins de la présente directive.

Les définitions suivantes sont aussi applicables :

a) ‘ utilisateur ’ : toute personne physique utilisant un service de communications électroniques accessible au public à des fins privées ou professionnelles sans être nécessairement abonnée à ce service;

b) ‘ données relatives au trafic ’ : toutes les données traitées en vue de l’acheminement d’une communication par un réseau de communications électroniques ou de sa facturation;

c) ‘ données de localisation ’ : toutes les données traitées dans un réseau de communications électroniques ou par un service de communications électroniques indiquant la position géographique de l’équipement terminal d’un utilisateur d’un service de communications électroniques accessible au public;

d) ‘ communication ’ : toute information échangée ou acheminée entre un nombre fini de parties au moyen d’un service de communications électroniques accessible au public. Cela ne comprend pas les informations qui sont acheminées dans le cadre d’un service de radiodiffusion au public par l’intermédiaire d’un réseau de communications électroniques, sauf dans la mesure où un lien peut être établi entre l’information et l’abonné ou utilisateur identifiable qui la reçoit;

f) le ‘ consentement ’ d’un utilisateur ou d’un abonné correspond au ‘ consentement de la personne concernée ’ figurant dans la directive 95/46/CE;

g) ‘ service à valeur ajoutée ’ : tout service qui exige le traitement de données relatives au trafic ou à la localisation, à l’exclusion des données qui ne sont pas indispensables pour la transmission d’une communication ou sa facturation;

h) ‘ courrier électronique ’ : tout message sous forme de texte, de voix, de son ou d’image envoyé par un réseau public de communications qui peut être stocké dans le réseau ou dans l’équipement terminal du destinataire jusqu’à ce que ce dernier le récupère.

i) ‘ violation de données à caractère personnel ’ : une violation de la sécurité entraînant accidentellement ou de manière illicite la destruction, la perte, l'altération, la divulgation ou l’accès non autorisés de données à caractère personnel transmises, stockées ou traitées d’une autre manière en relation avec la fourniture de services de communications électroniques accessibles au public dans la Communauté.

Article 3. Services concernés

1. La présente directive s’applique au traitement des données à caractère personnel dans le cadre de la fourniture de services de communications électroniques accessibles au public sur les réseaux de communications publics dans la Communauté, y compris les réseaux de

communications publics qui prennent en charge les dispositifs de collecte de données et d'identification.

[…]

Article 5. Confidentialité des communications

1. Les États membres garantissent, par la législation nationale, la confidentialité des communications effectuées au moyen d'un réseau public de communications et de services de communications électroniques accessibles au public, ainsi que la confidentialité des données relatives au trafic y afférentes. En particulier, ils interdisent à toute autre personne que les utilisateurs d'écouter, d'intercepter, de stocker les communications et les données relatives au trafic y afférentes, ou de les soumettre à tout autre moyen d'interception ou de surveillance, sans le consentement des utilisateurs concernés sauf lorsque cette personne y est légalement autorisée, conformément à l'article 15, paragraphe 1. Le présent paragraphe n'empêche pas le stockage technique nécessaire à l'acheminement d'une communication, sans préjudice du principe de confidentialité.

2. Le paragraphe 1 n'affecte pas l'enregistrement légalement autorisé de communications et des données relatives au trafic y afférentes, lorsqu'il est effectué dans le cadre des usages professionnels licites, afin de fournir la preuve d'une transaction commerciale ou de toute autre communication commerciale.

3. Les États membres garantissent que le stockage d'informations, ou l'obtention de l'accès à des informations déjà stockées, dans l'équipement terminal d'un abonné ou d'un utilisateur ne soit permise qu'à condition que l'abonné ou l'utilisateur, ait donné son accord, après avoir reçu, dans le respect de la directive 95/46/CE, une information claire et complète, entre autres sur les finalités du traitement. Cette disposition ne fait pas obstacle à un stockage ou à un accès techniques visant exclusivement à effectuer la transmission d'une communication par la voie d'un réseau de communications électroniques, ou strictement nécessaires au fournisseur pour la fourniture d'un service de la société de l'information expressément demandé par l'abonné ou l'utilisateur.

Article 6. Données relatives au trafic

1. Les données relatives au trafic concernant les abonnés et les utilisateurs traitées et stockées par le fournisseur d'un réseau public de communications ou d'un service de communications électroniques accessibles au public doivent être effacées ou rendues anonymes lorsqu'elles ne sont plus nécessaires à la transmission d'une communication sans préjudice des paragraphes 2, 3 et 5, du présent article ainsi que de l'article 15, paragraphe 1.

2. Les données relatives au trafic qui sont nécessaires pour établir les factures des abonnés et les paiements pour interconnexion peuvent être traitées. Un tel traitement n'est autorisé que jusqu'à la fin de la période au cours de laquelle la facture peut être légalement contestée ou des poursuites engagées pour en obtenir le paiement.

3. Afin de commercialiser des services de communications électroniques ou de fournir des services à valeur ajoutée, le fournisseur d'un service de communications électroniques accessible au public peut traiter les données visées au paragraphe 1 dans la mesure et pour la durée nécessaires à la fourniture ou à la commercialisation de ces services, pour autant que

l'abonné ou l'utilisateur que concernent ces données ait donné son consentement préalable. Les utilisateurs ou abonnés ont la possibilité de retirer à tout moment leur consentement pour le traitement des données relatives au trafic.

4. Le fournisseur de service doit informer l'abonné ou l'utilisateur des types de données relatives au trafic qui sont traités ainsi que de la durée de ce traitement aux fins visées au paragraphe 2 et, avant d'obtenir leur consentement, aux fins visées au paragraphe 3.

5. Le traitement des données relatives au trafic effectué conformément aux dispositions des paragraphes 1, 2, 3 et 4 doit être restreint aux personnes agissant sous l'autorité des fournisseurs de réseaux publics de communications et de services de communications électroniques accessibles au public qui sont chargées d'assurer la facturation ou la gestion du trafic, de répondre aux demandes de la clientèle, de détecter les fraudes et de commercialiser les services de communications électroniques ou de fournir un service à valeur ajoutée; ce traitement doit se limiter à ce qui est nécessaire à de telles activités.

6. Les paragraphes 1, 2, 3 et 5 s'appliquent sans préjudice de la possibilité qu'ont les organes compétents de se faire communiquer des données relatives au trafic conformément à la législation en vigueur dans le but de régler des litiges, notamment en matière d'interconnexion ou de facturation.

[…]

Article 9. Données de localisation autres que les données relatives au trafic

1. Lorsque des données de localisation, autres que des données relatives au trafic, concernant des utilisateurs ou abonnés de réseaux publics de communications ou de services de communications électroniques accessibles au public ou des abonnés à ces réseaux ou services, peuvent être traitées, elles ne le seront qu'après avoir été rendues anonymes ou moyennant le consentement des utilisateurs ou des abonnés, dans la mesure et pour la durée nécessaires à la fourniture d'un service à valeur ajoutée. Le fournisseur du service doit informer les utilisateurs ou les abonnés, avant d'obtenir leur consentement, du type de données de localisation autres que les données relatives au trafic qui sera traité, des objectifs et de la durée de ce traitement, et du fait que les données seront ou non transmises à un tiers en vue de la fourniture du service à valeur ajoutée. Les utilisateurs ou les abonnés ont la possibilité de retirer à tout moment leur consentement pour le traitement des données de localisation autres que les données relatives au trafic.

2. Lorsque les utilisateurs ou les abonnés ont donné leur consentement au traitement des données de localisation autres que les données relatives au trafic, ils doivent garder la possibilité d'interdire temporairement, par un moyen simple et gratuit, le traitement de ces données pour chaque connexion au réseau ou pour chaque transmission de communication.

3. Le traitement des données de localisation autres que les données relatives au trafic effectué conformément aux paragraphes 1 et 2 doit être restreint aux personnes agissant sous l'autorité du fournisseur du réseau public de communications ou service de communications

électroniques accessible au public ou du tiers qui fournit le service à valeur ajoutée, et doit se limiter à ce qui est nécessaire pour assurer la fourniture du service à valeur ajoutée.

[…]

Article 15. Application de certaines dispositions de la directive 95/46/CE

1. Les États membres peuvent adopter des mesures législatives visant à limiter la portée des droits et des obligations prévus aux articles 5 et 6, à l'article 8, paragraphes 1, 2, 3 et 4, et à l'article 9 de la présente directive lorsqu'une telle limitation constitue une mesure nécessaire, appropriée et proportionnée, au sein d'une société démocratique, pour sauvegarder la sécurité nationale - c'est-à-dire la sûreté de l'État - la défense et la sécurité publique, ou assurer la prévention, la recherche, la détection et la poursuite d'infractions pénales ou d'utilisations non autorisées du système de communications électroniques, comme le prévoit l'article 13, paragraphe 1, de la directive 95/46/CE. À cette fin, les États membres peuvent, entre autres, adopter des mesures législatives prévoyant la conservation de données pendant une durée limitée lorsque cela est justifié par un des motifs énoncés dans le présent paragraphe. Toutes les mesures visées dans le présent paragraphe sont prises dans le respect des principes généraux du droit communautaire, y compris ceux visés à l'article 6, paragraphes 1 et 2, du traité sur l'Union européenne.

1*bis*. Le paragraphe 1 n'est pas applicable aux données dont la conservation est spécifiquement exigée par la directive 2006/24/CE du Parlement européen et du Conseil du 15 mars 2006 sur la conservation de données traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communication aux fins visées à l'article 1er, paragraphe 1, de ladite directive.

1*ter*. Les fournisseurs établissent, sur la base des dispositions nationales adoptées au titre du paragraphe 1, des procédures internes permettant de répondre aux demandes d'accès aux données à caractère personnel concernant les utilisateurs. Ils mettent, sur demande, à la disposition de l'autorité nationale compétente des informations sur ces procédures, sur le nombre de demandes reçues, sur la base juridique invoquée et sur leur réponse.

2. Les dispositions du chapitre III de la directive 95/46/CE relatif aux recours juridictionnels, à la responsabilité et aux sanctions sont applicables aux dispositions nationales adoptées en application de la présente directive ainsi qu'aux droits individuels résultant de la présente directive.

3. Le groupe de protection des personnes à l'égard du traitement des données à caractère personnel, institué par l'article 29 de la directive 95/46/CE, remplit aussi les tâches visées à l'article 30 de ladite directive en ce qui concerne les matières couvertes par la présente directive, à savoir la protection des droits et des libertés fondamentaux ainsi que des intérêts légitimes dans le secteur des communications électroniques ».

En ce qui concerne la première branche du deuxième moyen

B.12. Dans la première branche du deuxième moyen, les parties requérantes font valoir que l'obligation d'identification généralisée et indifférenciée imposée par la loi attaquée à tous les utilisateurs finaux de services de communications électroniques constitue une ingérence dans le droit au respect de la vie privée qui va au-delà de ce qui est nécessaire au regard des objectifs poursuivis.

B.13.1. Le droit au respect de la vie privée n'est pas absolu. Les dispositions constitutionnelles et conventionnelles n'excluent pas une ingérence d'une autorité publique dans l'exercice du droit au respect de la vie privée, mais exigent que cette ingérence soit prévue par une disposition législative suffisamment précise, qu'elle réponde à un besoin social impérieux dans une société démocratique et qu'elle soit proportionnée à l'objectif légitime qu'elle poursuit.

Le législateur dispose en la matière d'une marge d'appréciation. Cette marge n'est toutefois pas illimitée : pour qu'une norme soit compatible avec le droit au respect de la vie privée, il faut que le législateur ait ménagé un juste équilibre entre tous les droits et intérêts en cause. Pour juger de cet équilibre, la Cour européenne des droits de l'homme tient compte notamment des dispositions de la Convention du Conseil de l'Europe du 28 janvier 1981 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel et de la recommandation n° R (87) 15 du Comité des ministres aux États membres visant à réglementer l'utilisation de données à caractère personnel dans le secteur de la police (CEDH, 25 février 1997, *Z c. Finlande*, § 95; grande chambre, 4 décembre 2008, *S. et Marper c. Royaume-Uni*, § 103).

B.13.2. Pour juger du caractère proportionné de mesures relatives au traitement de données à caractère personnel, il convient de tenir compte notamment de leur caractère automatisé, des techniques utilisées, de la précision, de la pertinence et du caractère excessif ou non des données traitées, de l'existence ou de l'absence de mesures qui limitent la durée de conservation des données, de l'existence ou de l'absence d'un système de contrôle indépendant permettant de vérifier si la conservation des données est encore requise, de la présence ou de l'absence de droits de contrôle et de voies de recours suffisants pour les personnes concernées,

de la présence ou de l'absence de garanties visant à éviter la stigmatisation des personnes dont les données sont traitées, du caractère distinctif de la réglementation et de la présence ou de l'absence de garanties visant à éviter l'usage inapproprié et abusif, par les services publics, des données à caractère personnel traitées (arrêt n° 108/2016 du 14 juillet 2016, B.12.2; arrêt n° 29/2018 du 15 mars 2018, B.14.4; arrêt n° 27/2020 du 20 février 2020, B.8.3; CEDH, grande chambre, 4 mai 2000, *Rotaru c. Roumanie*, § 59; décision, 29 juin 2006, *Weber et Saravia c. Allemagne*, § 135; 28 avril 2009, *K.H. e.a. c. Slovaquie*, §§ 60-69; grande chambre, 4 décembre 2008, *S. et Marper c. Royaume-Uni*, §§ 101-103, 119, 122 et 124; 18 avril 2013, *M.K. c. France*, §§ 37 et 42-44; 18 septembre 2014, *Brunet c. France*, §§ 35-37; 12 janvier 2016, *Szabó et Vissy c. Hongrie*, § 68; 30 janvier 2020, *Breyer c. Allemagne*, §§ 73-80; grande chambre, 25 mai 2021, *Centrum för rättvisa c. Suède*, §§ 262-278; grande chambre, 25 mai 2021, *Big Brother Watch c. Royaume-Uni*, §§ 348-364; CJUE, grande chambre, 8 avril 2014, C-293/12, *Digital Rights Ireland Ltd*, et C-594/12, *Kärntner Landesregierung e.a.*, points 56-66; grande chambre, 6 octobre 2020, C-511/18, C-512/18 et C-520/18, *La Quadrature du Net e.a.*, points 105-133; grande chambre, 6 octobre 2020, C-623/17, *Privacy International*, points 58-82; grande chambre, 2 mars 2021, C-746/18, *Prokuratuur*, points 50-56).

B.13.3. Il ressort de la jurisprudence de la Cour européenne des droits de l'homme que les données à caractère personnel ne peuvent pas être conservées plus longtemps que nécessaire pour la réalisation de la finalité pour laquelle elles ont été enregistrées sous une forme qui permette l'identification ou qui permette d'établir un lien entre une personne et des faits infractionnels. Pour apprécier la proportionnalité de la durée de conservation par rapport à l'objectif pour lequel les données ont été enregistrées, la Cour européenne des droits de l'homme tient compte de l'existence ou non d'un contrôle indépendant concernant la justification de la conservation des données dans les banques de données sur la base de critères précis, tels que la gravité des faits, le fait que la personne concernée a déjà fait l'objet dans le passé d'une arrestation, la force des soupçons qui pèsent sur une personne et toute autre circonstance particulière (CEDH, grande chambre, 4 décembre 2008, *S. et Marper c. Royaume-Uni*, § 103; 18 avril 2013, *M.K. c. France*, § 35; 17 décembre 2009, *B.B. c. France*, § 61; 18 septembre 2014, *Brunet c. France*, §§ 35-40).

B.14.1. En ce qui concerne la collecte, le traitement et la conservation généralisés et indifférenciés de données à caractère personnel des utilisateurs de réseaux de communication

électroniques, tant la Cour européenne des droits de l'homme que la Cour de justice font une distinction entre, d'une part, les données relatives au trafic et les données de localisation et, d'autre part, les données d'identification.

B.14.2. Elles considèrent la collecte, le traitement et la conservation de données relatives au trafic et de données de localisation de ces utilisateurs comme une très grave limitation du droit au respect de la vie privée, puisque de telles données sont susceptibles de révéler des informations sensibles sur un nombre important d'aspects de la vie privée des personnes concernées, comme leur orientation sexuelle, leurs opinions politiques, leurs convictions religieuses, philosophiques, sociétales ou autres et leur état de santé.

De telles données peuvent permettre de tirer des conclusions très précises sur la vie privée des personnes dont les données sont conservées, telles que leurs habitudes quotidiennes, leurs lieux de séjour permanents ou temporaires, leurs déplacements journaliers ou autres, leurs activités, leurs relations sociales et les milieux sociaux qu'elles fréquentent. Ces données fournissent les moyens d'établir un profil des personnes concernées, information tout aussi sensible que le contenu même de la communication (CEDH, grande chambre, 25 mai 2021, *Centrum för rättvisa c. Suède*, §§ 238-245; grande chambre, 25 mai 2021, *Big Brother Watch c. Royaume-Uni*, § 324-331; CJUE, grande chambre, 6 octobre 2020, C-511/18, C-512/18 et C-520/18, *La Quadrature du Net e.a.*, point 117; grande chambre, 6 octobre 2020, C-623/17, *Privacy International*, point 71).

La Cour de justice en déduit que la collecte, le traitement et la conservation généralisés et indifférenciés de données relatives au trafic et de données de localisation sont en principe interdits. Ils ne sont autorisés que pour des raisons de sécurité nationale et uniquement dans la mesure où il existe suffisamment d'indices concrets que l'État membre concerné fait face à une menace grave pour la sécurité nationale et que cette menace est réelle, actuelle et prévisible. En outre, cette conservation ne peut pas durer plus longtemps que strictement nécessaire par rapport à cette menace pour la sécurité nationale et doit être assortie de garanties strictes permettant de protéger efficacement les données à caractère personnel contre les risques d'abus, notamment à l'aide d'un contrôle effectif exercé par une juridiction ou par une entité administrative indépendante (CJUE, grande chambre, 6 octobre 2020, C-511/18, C-512/18 et C-520/18, *La Quadrature du Net e.a.*, points 137-139). En revanche, une collecte, un traitement et une conservation de données relatives au trafic et de données de localisation en vue de lutter

contre la criminalité grave ne peuvent pas avoir un caractère généralisé et indifférencié, mais doivent être délimités sur la base de critères géographiques ou liés à certaines personnes (*ibid.*, points 144-150).

Par contre, la Cour européenne des droits de l'homme n'interdit pas la collecte, le traitement et la conservation généralisés et indifférenciés de données relatives au trafic et de données de localisation, mais les soumet à un contrôle strict. Elle apprécie la légalité et la nécessité de telles mesures dans une société démocratique au regard des motifs pour lesquels l'interception en masse est ordonnée, des circonstances dans lesquelles les communications de personnes privées sont interceptées, de la procédure d'octroi d'une autorisation d'interception en masse, de la procédure à suivre pour la sélection du matériel à utiliser, des précautions qui sont prises si les données traitées sont communiquées à des tiers, des limites posées à la durée de l'interception et de la conservation des données à caractère personnel, en ce compris les circonstances dans lesquelles les données sont détruites, de la procédure et des modalités de contrôle *a priori* exercé par une autorité indépendante quant au respect des garanties, en ce compris la réparation ordonnée par cette autorité, et de la procédure de contrôle indépendant effectué *a posteriori* quant au respect de toutes les règles applicables (CEDH, grande chambre, 25 mai 2021, *Centrum för rättvisa c. Suède*, § 275; grande chambre, 25 mai 2021, *Big Brother Watch c. Royaume Uni*, § 361).

B.14.3. En revanche, la Cour européenne des droits de l'homme et la Cour de justice considèrent la collecte, le traitement et la conservation généralisés et indifférenciés de simples données d'identification d'utilisateurs de réseaux de communications électroniques comme une limitation moins grave du droit au respect de la vie privée, parce que ces données ne permettent pas, à elles seules, de connaître la date, l'heure, la durée et les destinataires d'une communication, ni l'endroit où cette communication a eu lieu ou la fréquence de communication avec certaines personnes pendant une période donnée. Ces données ne fournissent donc aucune information sur les communications données par ces personnes ni sur leur vie privée. Ces seules données ne permettent pas d'établir un profil de l'utilisateur ni de suivre ses mouvements (CEDH, 30 janvier 2020, *Breyer c. Allemagne*, §§ 92-95; CJUE, 2 octobre 2018, C-207/16, *Ministerio Fiscal*, point 62; grande chambre, 6 octobre 2020, C-511/18, C-512/18 et C-520/18, *La Quadrature du Net e.a.*, point 157).

La Cour de justice en déduit que le droit au respect de la vie privée ne s'oppose pas à une collecte, à un traitement et à une conservation généralisés et indifférenciés de données d'identification d'utilisateurs de réseaux de communications électroniques aux fins de la recherche, de la détection et de la poursuite d'infractions pénales ainsi que de la sauvegarde de la sécurité publique. À cet égard, il n'est pas nécessaire qu'il s'agisse d'infractions pénales graves ni de menaces ou d'atteintes graves à la sécurité publique (CJUE, grande chambre, 6 octobre 2020, C-511/18, C-512/18 et C-520/18, *La Quadrature du Net e.a.*, point 159). Par contre, il y a lieu de démontrer que « ces mesures assurent, par des règles claires et précises, que la conservation des données en cause est subordonnée au respect des conditions matérielles et procédurales y afférentes et que les personnes concernées disposent de garanties effectives contre les risques d'abus » (*ibid.*, point 168).

La Cour européenne des droits de l'homme contrôle la collecte, le traitement et la conservation généralisés et indifférenciés de ces données d'identification de manière moins intensive que la collecte, le traitement et la conservation de données relatives au trafic et de données de localisation. Elle vérifie tout d'abord si le délai de conservation est raisonnable, compte tenu de la durée habituelle d'une enquête pénale. En ce qui concerne l'accès aux données d'identification conservées, elle exige que les autorités qui peuvent consulter les données soient limitativement énumérées dans la réglementation applicable, que leur accès soit basé sur un fondement légal spécifique et clair dans le droit de la procédure pénale ou dans la législation relative aux services de renseignement et de sécurité et qu'elle soit justifiée par une suspicion concrète initiale. Dès que l'autorité n'a plus besoin des données d'identification demandées, elle doit les détruire immédiatement. La Cour européenne des droits de l'homme n'exige pas que l'intéressé soit informé de l'accès à ses données d'identification. Elle n'exige pas non plus qu'une supervision *a priori* soit organisée accéder à de simples données d'identification : un accès *a posteriori* à une instance judiciaire ou administrative indépendante, combiné aux recours de droit commun dont le prévenu dispose au cours d'un procès pénal, suffit (CEDH, 30 janvier 2020, *Breyer c. Allemagne*, §§ 96-107).

B.15.1. Par son arrêt n° 57/2021 du 22 avril 2021, la Cour a annulé les articles 2, b), 3 à 11 et 14 de la loi du 29 mai 2016 « relative à la collecte et à la conservation des données dans le secteur des communications électroniques » au motif qu'ils réglaient une collecte, un traitement et une conservation généralisés et indifférenciés tant de données d'identification que de données relatives au trafic et de données de localisation. La Cour a constaté que « la loi

attaquée [reposait], dans son principe même, sur une obligation de conservation généralisée et indifférenciée de l'ensemble des données visées à l'article 126, § 3, de la loi du 13 juin 2005, et qu'elle [poursuivait], d'une manière générale, […] des objectifs plus larges que la lutte contre la criminalité grave ou le risque d'atteinte à la sécurité publique » (B.17). En outre, la loi attaquée ne garantissait pas que la collecte, le traitement et la conservation de données relatives aux communications électroniques constituaient l'exception et non la règle, ni que l'accès à ces données était soumis à des règles claires et précises, que l'ingérence dans le droit au respect de la vie privée se limitait au strict nécessaire et que chaque ingérence répondait à des critères objectifs, établissant un rapport entre les données à conserver et le but poursuivi (B.18).

B.15.2. La loi présentement attaquée, en revanche, porte uniquement sur les données visées à l'article 127 de la loi du 13 juin 2005, à l'aide desquelles l'utilisateur final d'un service de communications électroniques fourni sur la base d'une carte de téléphonie mobile prépayée peut être identifié. L'article 12, alinéa 2, de l'arrêté royal du 27 novembre 2016 dispose que ces données d'identification peuvent varier en fonction de la méthode d'identification choisie, mais il énumère par la même occasion limitativement les données d'identification que l'entreprise concernée peut conserver au maximum :

« 1° le nom et le prénom;

2° le sexe;

3° la nationalité;

4° la date et le lieu de naissance;

5° l'adresse du domicile, l'adresse e-mail et le numéro de téléphone;

6° le numéro de registre national;

7° le numéro du document d'identité, le pays d'émission du document lorsqu'il s'agit d'un document étranger et la date de validité du document;

8° les références de l'opération de paiement conformément à l'article 17;

9° l'association de la carte prépayée au produit pour lequel l'utilisateur final est déjà identifié conformément à l'article 18;

10° la photo de l'utilisateur final, mais uniquement pour les documents autres que la carte d'identité électronique belge ».

Compte tenu de l'annulation partielle visée en B.9.1 et du maintien des effets visé en B.9.3, le législateur doit, avant la date mentionnée dans le dispositif, inclure dans une disposition législative les données d'identification et les documents d'identification qui peuvent servir à l'application de l'article 127 de la loi du 13 juin 2005.

B.15.3. Ces données personnelles ne sont pas des données relatives au trafic et des données de localisation, mais uniquement les données qui sont habituellement utilisées pour identifier une personne. Il n'est pas possible, à l'aide de ces seules données, de suivre les déplacements, les communications, les activités ou les relations sociales de cette personne, ni d'établir un profil personnel permettant de tirer des conclusions précises sur son orientation sexuelle, ses convictions et son état de santé. En soi, elles ne divulguent donc pas d'informations sensibles sur la vie privée.

Il est exact que ces données d'identification peuvent ensuite être associées à d'autres données et contribuer, de cette manière, à la divulgation de telles informations sensibles sur la vie privée d'une personne. Ces autres données doivent toutefois, dans ce cas, être collectées d'une autre manière et cette collecte doit elle aussi s'effectuer dans le respect de la législation applicable et des droits fondamentaux de l'intéressé.

Par conséquent, il y a lieu d'apprécier la compatibilité de la loi attaquée avec le droit au respect de la vie privée à l'aide des critères mentionnés en B.14.3.

B.16.1. Les conditions matérielles et procédurales de la collecte, du traitement et de la conservation des données d'identification des utilisateurs finaux d'un réseau de communications électroniques sur la base d'une carte de téléphonie mobile prépayée sont réglées dans les articles 126 et 127 de la loi du 13 juin 2005 et dans les arrêtés royaux du 19 septembre 2013 et du 27 novembre 2016.

B.16.2. Comme il est dit en B.2.1 à B.2.7, l'article 127 de la loi du 13 juin 2005 détermine les personnes qui se voient imposer des obligations dans ce cadre, à savoir les opérateurs, les fournisseurs, les canaux de vente de services de communications électroniques, les entreprises qui fournissent un service d'identification et les utilisateurs finaux eux-mêmes. Il désigne également le responsable du traitement des données, à savoir l'opérateur ou le fournisseur. Il définit en outre le principe selon lequel tous les utilisateurs finaux doivent être identifiables,

indépendamment du fait qu'ils utilisent une ancienne ou une nouvelle carte de téléphonie mobile prépayée, et dispose que l'identification doit être effectuée sur la base d'un document d'identification comprenant le numéro de registre national.

L'arrêté royal du 27 novembre 2016 oblige les utilisateurs finaux de cartes de téléphonie mobile prépayées à s'identifier auprès de l'opérateur au plus tard lors de l'activation de celles-ci selon l'une des méthodes d'identification valides décrites dans le même arrêté royal et à l'aide d'un des documents d'identification valides mentionnés dans l'arrêté royal. Il a obligé les opérateurs à identifier tous les utilisateurs finaux d'anciennes cartes de téléphonie mobile prépayées avant le 7 juin 2017 et leur interdit d'encore activer de nouvelles cartes prépayées si l'utilisateur final n'a pas encore été identifié. S'ils sont informés par l'utilisateur final de la perte ou du vol de la carte de téléphonie mobile prépayée, ils doivent la rendre immédiatement inutilisable.

En ce qui concerne le traitement des données proprement dit, l'arrêté royal du 27 novembre 2016 dispose que l'opérateur, le fournisseur d'un service d'identification ou le canal de vente de services de communication électroniques lisent électroniquement la carte d'identité électronique belge, en font un scan, une photo ou une copie, en ce compris de la photo se trouvant sur cette carte et du numéro de cette carte. Avant l'activation de la carte de téléphonie mobile prépayée, l'opérateur doit contrôler si la carte d'identité présentée a été volée ou a fait l'objet d'une fraude. Il doit également conserver la méthode d'identification qui a été utilisée pour identifier l'utilisateur final pendant la durée visée à l'article 126 de la loi du 13 juin 2015.

B.16.3. Les parties requérantes ne contestent pas que ces règles sont claires et précises. Elles font seulement valoir que le cadre légal relatif à la conservation des données traitées manque de clarté depuis l'arrêt de la Cour n° 57/2021 du 22 avril 2021, parce que la Cour a annulé dans cet arrêt les règles relatives aux données traitées, aux personnes impliquées dans le traitement, aux conditions et aux finalités du traitement, ainsi que les règles relatives à la Cellule de coordination. De ce fait, il n'existerait plus de conditions matérielles et procédurales réglant le traitement des données ou des documents d'identification conservés.

B.16.4. Comme il est dit en B.8.7.3, l'arrêt n° 57/2021 n'a pas pour effet qu'il n'existe plus de cadre législatif pour la conservation des données d'identification collectées et traitées.

L'annulation des articles 2, b), 3 à 11 et 14 de la loi du 29 mai 2016 a seulement pour effet que l'article 126 de la loi du 13 juin 2005 est actuellement applicable, pour ce qui est des données d'identification des utilisateurs de cartes prépayées, dans sa version qui a été modifiée pour la dernière fois par l'article 33 de la loi du 4 février 2010 « relative aux méthodes de recueil des données par les services de renseignement et de sécurité ».

B.16.5. En application de l'article 126 de la loi du 13 juin 2005, l'arrêté royal du 19 septembre 2013 fixe les conditions de conservation des données collectées. Les articles 3 à 6 de cet arrêté déterminent les données qui doivent être conservées et les personnes qui se chargent de la conservation :

« Art. 3. § 1er. Pour ce qui concerne les données relatives à l'identification de l'utilisateur final, de l'équipement terminal qui est présumé avoir été utilisé et du service de communications électroniques utilisé, les fournisseurs de services de téléphonie fixe accessibles au public et les fournisseurs de réseaux publics de communications électroniques sous-jacents conservent les données suivantes :

1° le numéro attribué à l'utilisateur final;

2° les données personnelles de l'utilisateur final;

3° la date de début de l'abonnement ou de l'enregistrement au service;

4° le type de service de téléphonie fixe utilisé ainsi que les services annexes auxquels l'utilisateur final a souscrit;

5° en cas de transfert du numéro de l'utilisateur final auprès d'un autre fournisseur, l'identité du fournisseur qui transfère le numéro et l'identité du fournisseur auquel le numéro est transféré;

6° les données relatives au type de paiement, à l'identification du moyen de paiement et à la date du paiement de l'abonnement ou de l'utilisation du service.

§ 2. Pour ce qui concerne les données relatives au trafic et à la localisation, les fournisseurs de services de téléphonie fixe accessibles au public et les fournisseurs de réseaux publics de communications électroniques sous-jacents conservent les données suivantes :

1° l'identification du numéro de téléphone de l'appelant et de l'appelé;

2° la localisation du point de terminaison du réseau de l'appelant et de l'appelé;

3° en cas d'appel multiple, de déviation ou de renvoi, l'identification de toutes les lignes en ce compris, celles vers lesquelles l'appel a été transféré;

4° la date et l'heure exacte du début et de la fin de l'appel;

5° la description du service de téléphonie utilisé.

§ 3. Les données visées au paragraphe 1er sont soumises à l'article 126, § 3, alinéa 1er, de la loi.

Les données visées au paragraphe 2 sont soumises à l'article 126, § 3, alinéa 2, de la loi.

Art. 4. § 1er. Pour ce qui concerne les données relatives à l'identification de l'utilisateur final, de l'équipement terminal qui est présumé avoir été utilisé et du service de communications électroniques utilisé, les fournisseurs d'un service de téléphonie mobile accessible au public et les fournisseurs de réseaux publics de communications électroniques sous-jacents conservent les données suivantes :

1° le numéro attribué à l'utilisateur final ainsi que l'identité internationale d'abonné mobile (' International Mobile Subscriber Identity ', ' IMSI ');

2° les données personnelles de l'utilisateur final;

3° la date et le lieu de la souscription à l'abonnement ou de l'enregistrement de l'utilisateur final;

4° la date et l'heure de la première activation du service, ainsi que l'identifiant cellulaire à partir duquel le service a été activé;

5° les services annexes auxquels l'utilisateur final a souscrit;

6° en cas de transfert de numéro auprès d'un autre opérateur, l'identité de l'opérateur d'origine de l'utilisateur final;

7° les données relatives au type de paiement, à l'identification du moyen de paiement et à la date du paiement de l'abonnement ou de l'utilisation du service;

8° le numéro d'identification du terminal mobile de l'utilisateur final (' International Mobile Equipment Identity ', ' IMEI ').

§ 2. Pour ce qui concerne les données relatives au trafic et à la localisation, les fournisseurs d'un service de téléphonie mobile accessible au public et les fournisseurs de réseaux publics de communications électroniques sous-jacents conservent les données suivantes :

1° l'identification du numéro de téléphone de l'appelant et de l'appelé;

2° en cas d'appel multiple, de déviation ou de renvoi, l'identification de toutes les lignes en ce compris, celles vers lesquelles l'appel a été transféré;

3° l'identité internationale d'abonné mobile (' International Mobile Subscriber Identity ', ' IMSI ') de l'appelant et de l'appelé;

4° l'identité internationale d'équipement mobile (' International Mobile Equipment Identity ', ' IMEI ') du terminal mobile de l'appelant et de l'appelé;

5° la date et l'heure exacte du début et de la fin de l'appel;

6° la localisation du point de terminaison du réseau au début et à la fin de chaque connexion;

7° les données permettant d'établir la localisation géographique des cellules en se référant à leur identifiant cellulaire au moment où la communication a été effectuée;

8° les caractéristiques techniques du service de téléphonie utilisé.

§ 3. Les données visées au paragraphe 1er sont soumises à l'article 126, § 3, alinéa 1er, de la loi.

Les données visées au paragraphe 2 sont soumises à l'article 126, § 3, alinéa 2, de la loi.

Art. 5. § 1er. Pour ce qui concerne les données relatives à l'identification de l'utilisateur final, de l'équipement terminal qui est présumé avoir été utilisé et du service de communications électroniques utilisé, les fournisseurs de service d'accès à l'internet accessible au public et les fournisseurs de réseaux publics de communications électroniques sous-jacents conservent les données suivantes :

1° l'identifiant de l'utilisateur final;

2° les données personnelles de l'utilisateur final;

3° la date et l'heure de la souscription à l'abonnement ou de l'enregistrement de l'utilisateur final;

4° l'adresse IP et le port source de la connexion ayant servi à la création de l'abonnement ou à l'enregistrement de l'utilisateur final;

5° l'identification du point de terminaison du réseau ayant servi à la création de l'abonnement ou de l'inscription en tant qu'utilisateur final;

6° les services annexes auxquels l'utilisateur final a souscrit auprès du prestataire d'accès Internet public concerné;

7° les données relatives au type de paiement, à l'identification du moyen de paiement et à la date du paiement de l'abonnement ou de l'utilisation du service.

§ 2. Pour ce qui concerne les données relatives au trafic et à la localisation, les fournisseurs de service d'accès à l'internet accessible au public et les fournisseurs de réseaux publics de communications électroniques sous-jacents conservent les données suivantes :

1° l'identifiant de l'utilisateur final;

2° a) l'adresse IP;

b) en cas d'utilisation partagée d'une adresse IP, les ports attribués de l'adresse IP ainsi que la date et l'heure de l'attribution;

3° l'identification et la localisation du point de terminaison du réseau utilisé par l'utilisateur final au début et à la fin d'une connexion;

4° la date et l'heure de l'ouverture et de la fermeture d'une session du service d'accès à l'internet;

5° le volume de données envoyées vers le réseau et téléchargées pendant la durée de la session ou autre unité de temps demandée;

6° les données permettant d'établir la localisation géographique des cellules en se référant à leur identifiant cellulaire au moment où la communication a été effectuée.

§ 3. Les données visées au paragraphe 1er sont soumises à l'article 126, § 3, alinéa 1er, de la loi.

Les données visées au paragraphe 2 sont soumises à l'article 126, § 3, alinéa 2, de la loi .

Art. 6. § 1er. Pour ce qui concerne les données relatives à l'identification de l'utilisateur final, de l'équipement terminal qui est présumé avoir été utilisé et du service de communications électroniques utilisé, les fournisseurs d'un service de courrier électronique par internet accessible au public, les fournisseurs d'un service de téléphonie par internet accessible au public et les fournisseurs de réseaux publics de communications électroniques sous-jacents conservent les données suivantes :

1° l'identifiant de l'utilisateur final;

2° les données personnelles de l'utilisateur final;

3° la date et l'heure de la création du compte de courrier électronique ou de téléphonie par internet;

4° l'adresse IP et le port source ayant servi à la création du compte de courrier électronique ou de téléphonie par l'internet;

5° les données relatives au type de paiement, à l'identification du moyen de paiement et à la date du paiement de l'abonnement ou de l'utilisation du service.

§ 2. Pour ce qui concerne les données relatives au trafic et à la localisation, les fournisseurs d'un service de courrier électronique par internet accessible au public, les fournisseurs d'un service de téléphonie par internet accessible au public et les fournisseurs de réseaux publics de communications électroniques sous-jacents conservent les données suivantes :

1° l'identifiant de l'utilisateur final du compte de courrier électronique ou de téléphonie par internet, ainsi que le numéro ou l'identifiant du destinataire prévu de la communication;

2° le numéro de téléphone attribué à toute communication entrant dans le réseau téléphonique public dans le cadre d'un service téléphonique par internet;

3° a) l'adresse IP et le port source utilisés par l'utilisateur final;

b) l'adresse IP et le port source utilisés par le destinataire;

4° la date et l'heure de l'ouverture et de la fermeture d'une session du service de courrier électronique ou de téléphonie par internet;

5° la date et l'heure de la connexion établie à l'aide du compte de téléphonie par Internet;

6° les caractéristiques techniques du service utilisé.

§ 3. Les données visées au paragraphe 1er sont soumises à l'article 126, § 3, alinéa 1er, de la loi.

Les données visées au paragraphe 2 sont soumises à l'article 126, § 3, alinéa 2, de la loi ».

B.16.6. Cet arrêté royal ne fixe toutefois pas de délai de conservation minimal ou maximal des données d'identification traitées en vertu de l'article 127 de la loi du 13 juin 2005. En effet, ce délai était ancré dans l'article 126, § 3, de la loi du 13 juin 2005, annulé par l'arrêt n° 57/2021, qui disposait :

« Les données visant à identifier l'utilisateur ou l'abonné et les moyens de communication, à l'exclusion des données spécifiquement prévues aux alinéas 2 et 3, sont conservées pendant douze mois à compter de la date à partir de laquelle une communication est possible pour la dernière fois à l'aide du service utilisé.

Les données relatives à l'accès et la connexion de l'équipement terminal au réseau et au service et à la localisation de cet équipement, y compris le point de terminaison du réseau, sont conservées pendant douze mois à partir de la date de la communication.

Les données de communication, à l'exclusion du contenu, en ce compris leur origine et leur destination, sont conservées pendant douze mois à partir de la date de la communication.

Le Roi fixe, par arrêté délibéré en Conseil des ministres, sur proposition du ministre de la Justice et du ministre, et après avis de la Commission de la protection de la vie privée et de l'Institut, les données à conserver par type de catégories visées aux alinéas 1 à 3 ainsi que les exigences auxquelles ces données doivent répondre ».

Dans l'attente de l'entrée en vigueur d'une nouvelle version de l'article 126 de la loi du 13 juin 2005, l'utilisateur final d'une carte de téléphonie mobile prépayée n'est toutefois pas soumis à un risque de conservation illimitée de ses données d'identification. En effet, la version actuellement applicable de cette disposition mentionne un délai de conservation maximal de trente-six mois.

Par ailleurs, cet utilisateur final bénéficie de la protection du RGPD, que le responsable du traitement se doit de respecter parallèlement aux dispositions applicables du droit national – et, si nécessaire, en priorité par rapport à celles-ci. En vertu du principe de la limitation de la conservation inscrit dans l'article 5, point e), du RGPD, le responsable du traitement doit conserver les données personnelles « sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées ».

Compte tenu de ces dispositions, il peut être admis, dans l'attente de l'entrée en vigueur d'un nouveau cadre législatif en matière de conservation des données, que la législation applicable ne prévoie temporairement pas un délai de conservation spécifique. Dans cette période intermédiaire, il appartient aux juridictions et aux autorités administratives compétentes de garantir, en vertu de ces dispositions, que les données d'identification des utilisateurs finaux de cartes de téléphonie mobile prépayées ne sont pas conservées plus longtemps que ce qui est nécessaire au regard des objectifs poursuivis par l'obligation d'identification attaquée.

B.16.7. Ces objectifs sont énumérés limitativement dans l'article 127, § 1er, de la loi du 13 juin 2005. Il s'agit du bon fonctionnement des services d'urgence, de l'instruction pénale et du fonctionnement des services de renseignement et de sécurité. Ces deuxième et troisième objectifs correspondent aux motifs pour lesquels la Cour de justice autorise la conservation des données d'identification (CJUE, grande chambre, 6 octobre 2020, *La Quadrature du Net e.a.*, C-511/18, C-512/18 et C-520/18, points 152 à 159). Le bon fonctionnement des services d'urgence, quant à lui, est lié aux obligations positives qui incombent aux autorités dans le cadre des droits que les victimes d'infractions et d'accidents puisent dans les articles 2, 3, 5 et 8 de la Convention européenne des droits de l'homme.

B.16.8.1. La législation relative à ces services mentionne en outre de manière limitative les autorités qui ont accès aux données d'identification conservées ainsi que les conditions matérielles et procédurales qu'elles doivent remplir à cette fin.

B.16.8.2. L'accès à ces données dans le cadre d'une information pénale et d'une instruction pénale est réglé par les articles 46*bis*, 88*bis* et 90*ter* à 90*decies* du Code d'instruction criminelle.

L'article 46*bis* du Code d'instruction criminelle dispose :

« § 1er. En recherchant les crimes et les délits, le procureur du Roi peut, par une décision motivée et écrite, procéder ou faire procéder sur la base de toutes données détenues par lui, ou au moyen d'un accès aux fichiers des clients des acteurs visés à l'alinéa 2, premier et deuxième tirets, à :

1° l'identification de l'abonné ou de l'utilisateur habituel d'un service visé à l'alinéa 2, deuxième tiret, ou bien du moyen de communication électronique utilisé;

2° l'identification des services visés à l'alinéa 2, deuxième tiret, auxquels une personne déterminée est abonnée ou qui sont habituellement utilisés par une personne déterminée.

Si nécessaire, il peut pour ce faire requérir, directement ou par l'intermédiaire du service de police désigné par le Roi, la collaboration :

- de l'opérateur d'un réseau de communications électroniques, et

- de toute personne qui met à disposition ou offre, sur le territoire belge, d'une quelconque manière, un service qui consiste à transmettre des signaux via des réseaux de communications électroniques ou à autoriser des utilisateurs à obtenir, recevoir ou diffuser des informations via un réseau de communications électroniques. Est également compris le fournisseur d'un service de communications électroniques.

La motivation reflète le caractère proportionnel eu égard au respect de la vie privée et subsidiaire à tout autre devoir d'enquête.

En cas d'extrême urgence, le procureur du Roi peut ordonner verbalement cette mesure.

La décision est confirmée par écrit dans les plus brefs délais.

Pour des infractions qui ne sont pas de nature à entraîner un emprisonnement correctionnel principal d'un an ou une peine plus lourde, le procureur du Roi ne peut requérir les données visées à l'alinéa 1er que pour une période de six mois préalable à sa décision.

§ 2. Les acteurs visés au § 1er, alinéa 2, 1er et 2e tirets, requis de communiquer les données visées au paragraphe 1er communiquent au procureur du Roi ou à l'officier de police

judiciaire les données en temps réel ou, le cas échéant, au moment précisé dans la réquisition, selon les modalités fixées par le Roi, sur proposition du ministre de la Justice et du ministre compétent pour les Télécommunications.

Le Roi fixe, après avis de la Commission de la protection de la vie privée et sur proposition du Ministre de la Justice et du Ministre compétent pour les Télécommunications, les conditions techniques d'accès aux données visées au § 1er et disponibles pour le procureur du Roi et le service de police désigné au même paragraphe.

Toute personne qui, du chef de sa fonction, a connaissance de la mesure ou y prête son concours, est tenue de garder le secret. Toute violation du secret est punie conformément à l'article 458 du Code pénal.

Toute personne qui refuse de communiquer les données ou qui ne les communique pas en temps réel ou, le cas échéant, au moment précisé dans la réquisition est punie d'une amende de vingt-six euros à dix mille euros ».

L'article 88*bis* du Code d'instruction criminelle dispose :

« § 1er. S'il existe des indices sérieux que les infractions sont de nature à entraîner un emprisonnement correctionnel principal d'un an ou une peine plus lourde, et lorsque le juge d'instruction estime qu'il existe des circonstances qui rendent le repérage de communications électroniques ou la localisation de l'origine ou de la destination de communications électroniques nécessaire à la manifestation de la vérité, il peut faire procéder :

1° au repérage des données de trafic de moyens de communication électronique à partir desquels ou vers lesquels des communications électroniques sont adressées ou ont été adressées;

2° à la localisation de l'origine ou de la destination de communications électroniques.

Si nécessaire, il peut pour ce faire requérir, directement ou par l'intermédiaire du service de police désigné par le Roi, la collaboration :

- de l'opérateur d'un réseau de communications électroniques; et

- de toute personne qui met à disposition ou offre, sur le territoire belge, d'une quelconque manière, un service qui consiste à transmettre des signaux via des réseaux de communications électroniques ou à autoriser des utilisateurs à obtenir, recevoir ou diffuser des informations via un réseau de communications électroniques. Est également compris le fournisseur d'un service de communications électroniques.

Dans les cas visés à l'alinéa 1er, pour chaque moyen de communication électronique dont les données de trafic sont repérées ou dont l'origine ou la destination de la communication électronique est localisée, le jour, l'heure, la durée et, si nécessaire, le lieu de la communication électronique sont indiqués et consignés dans un procès-verbal.

Le juge d'instruction indique les circonstances de fait de la cause qui justifient la mesure, son caractère proportionnel eu égard au respect de la vie privée et subsidiaire à tout autre devoir d'enquête, dans une ordonnance motivée.

Il précise également la durée durant laquelle la mesure pourra s'appliquer pour le futur, cette durée ne pouvant excéder deux mois à dater de l'ordonnance, sans préjudice de renouvellement et, le cas échéant, la période pour le passé sur laquelle l'ordonnance s'étend conformément au paragraphe 2.

En cas de flagrant délit, le procureur du Roi peut ordonner la mesure pour les infractions visées à l'article 90*ter*, §§ 2, 3 et 4. Dans ce cas, la mesure doit être confirmée dans les vingt-quatre heures par le juge d'instruction.

S'il s'agit toutefois de l'infraction visée à l'article 137, 347*bis*, 434 ou 470 du Code pénal, à l'exception de l'infraction visée à l'article 137, § 3, 6°, du même Code, le procureur du Roi peut ordonner la mesure tant que la situation de flagrant délit perdure, sans qu'une confirmation par le juge d'instruction ne soit nécessaire.

S'il s'agit de l'infraction visée à l'article 137 du Code pénal, à l'exception de l'infraction visée à l'article 137, § 3, 6°, du même Code, le procureur du Roi peut en outre ordonner la mesure dans les septante-deux heures suivant la découverte de cette infraction, sans qu'une confirmation par le juge d'instruction soit nécessaire.

Toutefois, le procureur du Roi peut ordonner la mesure si le plaignant le sollicite, lorsque cette mesure s'avère indispensable à l'établissement d'une infraction visée à l'article 145, § 3 et § 3*bis* de la loi du 13 juin 2005 relative aux communications électroniques.

En cas d'urgence, la mesure peut être ordonnée verbalement. Elle doit être confirmée dans les plus brefs délais dans la forme prévue aux alinéas 4 et 5.

§ 2. Pour ce qui concerne l'application de la mesure visée au paragraphe 1er, alinéa 1er, aux données de trafic ou de localisation conservées sur la base de l'article 126 de la loi du 13 juin 2005 relative aux communications électroniques, les dispositions suivantes s'appliquent :

- pour une infraction visée au livre II, titre I*ter*, du Code pénal, le juge d'instruction peut dans son ordonnance requérir les données pour une période de douze mois préalable à l'ordonnance;

- pour une autre infraction visée à l'article 90*ter*, §§ 2 à 4, qui n'est pas visée au premier tiret ou pour une infraction qui est commise dans le cadre d'une organisation criminelle visée à l'article 324*bis* du Code pénal, ou pour une infraction qui est de nature à entraîner un emprisonnement correctionnel principal de cinq ans ou une peine plus lourde, le juge d'instruction peut dans son ordonnance requérir les données pour une période de neuf mois préalable à l'ordonnance;

- pour les autres infractions, le juge d'instruction ne peut requérir les données que pour une période de six mois préalable à l'ordonnance.

§ 3. La mesure ne peut porter sur les moyens de communication électronique d'un avocat ou d'un médecin que si celui-ci est lui-même soupçonné d'avoir commis une infraction visée au paragraphe 1er ou d'y avoir participé, ou si des faits précis laissent présumer que des tiers soupçonnés d'avoir commis une infraction visée au paragraphe 1er, utilisent ses moyens de communication électronique.

La mesure ne peut être exécutée sans que le bâtonnier ou le représentant de l'ordre provincial des médecins, selon le cas, en soit averti. Ces mêmes personnes seront informées par le juge d'instruction des éléments qu'il estime relever du secret professionnel. Ces éléments ne sont pas consignés au procès-verbal. Ces personnes sont tenues au secret. Toute violation du secret est punie conformément à l'article 458 du Code pénal.

§ 4. Les acteurs visés au § 1er, alinéa 2, communiquent les informations demandées en temps réel ou, le cas échéant, au moment précisé dans la réquisition, selon les modalités fixées par le Roi, sur la proposition du ministre de la Justice et du ministre compétent pour les Télécommunications.

Toute personne qui, du chef de sa fonction, a connaissance de la mesure ou y prête son concours, est tenue de garder le secret. Toute violation du secret est punie conformément à l'article 458 du Code pénal.

Toute personne qui refuse de prêter son concours technique aux réquisitions visées au présent article, concours dont les modalités sont fixées par le Roi, sur la proposition du ministre de la Justice et du ministre compétent pour les Télécommunications, ou ne le prête pas en temps réel ou, le cas échéant, au moment précisé dans la réquisition, est punie d'une amende de vingt-six euros à dix mille euros ».

L'article 90*ter*, § 1er, du Code d'instruction criminelle dispose :

« Sans préjudice de l'application des articles 39*bis*, 87, 88, 89*bis* et 90, le juge d'instruction peut, dans un but secret, intercepter, prendre connaissance, explorer et enregistrer, à l'aide de moyens techniques, des communications non accessibles au public ou des données d'un système informatique ou d'une partie de celui-ci, ou étendre la recherche dans un système informatique ou une partie de celui-ci.

Cette mesure ne peut être ordonnée que dans des cas exceptionnels, lorsque les nécessités de l'instruction l'exigent, s'il existe des indices sérieux que cela concerne une infraction visée au paragraphe 2, et si les autres moyens d'investigation ne suffisent pas à la manifestation de la vérité.

En vue de permettre cette mesure, le juge d'instruction peut également, à l'insu ou sans le consentement de l'occupant, du propriétaire ou de son ayant droit, ou de l'utilisateur, ordonner, à tout moment :

- la pénétration dans un domicile, un lieu privé ou un système informatique;

- la suppression temporaire de toute protection des systèmes informatiques concernés, le cas échéant à l'aide de moyens techniques, de faux signaux, de fausses clés ou de fausses qualités;

- l'installation de dispositifs techniques dans les systèmes informatiques concernés en vue du décryptage et du décodage de données stockées, traitées ou transmises par ce système.

La mesure visée au présent paragraphe ne peut être ordonnée que pour rechercher les données qui peuvent servir à la manifestation de la vérité. Elle ne peut être ordonnée qu'à l'égard soit de personnes soupçonnées, sur la base d'indices précis, d'avoir commis l'infraction, soit à l'égard des moyens de communication ou systèmes informatiques régulièrement utilisés par un suspect, soit à l'égard des lieux présumés fréquentés par celui-ci. Elle peut également être ordonnée à l'égard de personnes présumées, sur la base de faits précis, être en communication régulière avec un suspect ».

B.16.8.3. L'accès à ces données dans le cadre d'une enquête réalisée par les services de renseignement et de sécurité est réglé par l'article 16/2, § 1er, de la loi du 30 novembre 1998, qui dispose :

« Les services de renseignement et de sécurité peuvent, dans l'intérêt de l'exercice de leurs missions, requérir le concours d'un opérateur de réseaux de communications électroniques ou d'un fournisseur de services de communications électroniques pour procéder à :

1° l'identification de l'abonné ou de l'utilisateur habituel d'un service de communication électronique ou du moyen de communication électronique utilisé;

2° l'identification des services et des moyens de communications électroniques auxquels une personne déterminée est abonnée ou qui sont habituellement utilisés par une personne déterminée.

La réquisition est effectuée par écrit par le dirigeant de service ou son délégué. En cas d'urgence, le dirigeant de service ou son délégué peut requérir ces données verbalement. Cette réquisition verbale est confirmée dans un délai de vingt-quatre heures par une réquisition écrite.

Tout opérateur d'un réseau de communications électroniques et tout fournisseur d'un service de communications électroniques qui est requis donne au dirigeant de service ou à son délégué les données qui ont été demandées dans un délai et selon les modalités à fixer par un arrêté royal pris sur la proposition du ministre de la Justice, du ministre de la Défense et du ministre qui a les communications électroniques dans ses attributions.

Le dirigeant de service ou son délégué peut, dans le respect des principes de proportionnalité et de subsidiarité, et moyennant l'enregistrement de la consultation, également obtenir les données visées au moyen d'un accès aux fichiers des clients de l'opérateur ou du fournisseur du service. Le Roi fixe, sur la proposition du ministre de la Justice, du ministre de la Défense et du ministre qui a les communications électroniques dans ses attributions, les conditions techniques auxquelles cet accès est possible ».

B.16.8.4. L'accès à ces données par les services d'urgence est réglé par l'article 107, § 2, de la loi du 13 juin 2005, qui dispose :

« Les opérateurs concernés par un appel d'urgence vers un service d'urgence offrant de l'aide sur place, si nécessaire en se coordonnant entre eux, fournissent aux centrales de gestion de ce service d'urgence, dès que l'appel leur parvient et gratuitement, les données d'identification de l'appelant.

Cette obligation est également d'application lorsque les centrales de gestion des services d'urgence offrant de l'aide sur place sont exploitées par une organisation qui est chargée de cette tâche par les pouvoirs publics.

Les coûts d'investissement et d'exploitation relatifs aux bases de données des données d'identification de l'appelant et aux lignes d'accès utilisées par les services d'urgence pour consulter ces bases de données sont à charge des opérateurs.

Si un opérateur offre ses propres services commerciaux pour la fourniture de données de localisation aux abonnés, alors la précision des données de localisation qui font partie de l'identification de l'appelant lors d'un appel d'urgence et qui doivent être fournies aux services d'urgence offrant de l'aide sur place conformément au présent paragraphe et la vitesse à laquelle elles sont transmises au service d'urgence concerné doivent être au moins égales à la meilleure qualité offerte au niveau commercial par cet opérateur. L'Institut peut définir, en concertation avec les services d'urgence concernés, les critères relatifs à la précision et la fiabilité des données de localisation de l'appelant fournies.

L'identification de l'appelant peut être utilisée par les services d'urgence offrant de l'aide sur place ou par l'organisation qui est chargée de l'exploitation des centrales de gestion des services d'urgence par les pouvoirs publics, à l'aide de mesures administratives et techniques approuvées par le ministre sur l'avis de l'Institut et de la Commission pour la protection de la vie privée, afin de lutter contre les appels malveillants ou l'utilisation abusive des numéros d'urgence. Ces mesures ne peuvent toutefois entraîner une inaccessibilité du numéro d'urgence du service d'urgence en question à partir d'une connexion bien précise pendant une période ininterrompue excédant vingt-quatre heures.

Les centrales de gestion des services d'urgence offrant de l'aide à distance obtiennent gratuitement des opérateurs concernés l'identification de la ligne appelante disponible sur le réseau des opérateurs, afin de pouvoir traiter des appels d'urgence et de lutter contre les appels malveillants, même si l'utilisateur a entrepris des démarches pour empêcher l'envoi de l'identification. Le format d'identification de la ligne appelante fournie doit être conforme aux

normes ETSI applicables et est défini par l'Institut en concertation avec les services d'urgence et les opérateurs.

L'identification de la ligne appelante peut être utilisée par les services d'urgence offrant de l'aide à distance, à l'aide de mesures administratives et techniques approuvées par le ministre sur l'avis de l'Institut et de la Commission pour la protection de la vie privée, afin de lutter contre les appels malveillants. Ces mesures ne peuvent toutefois entraîner une inaccessibilité du numéro d'urgence du service d'urgence en question à partir d'une connexion bien précise pendant une période ininterrompue excédant vingt-quatre heures ».

B.16.8.5. Ces dispositions règlent de manière claire et précise les conditions matérielles et procédurales auxquelles ces autorités peuvent avoir accès aux données d'identification traitées en vertu de l'article 127 de la loi du 13 juin 2005.

Lorsqu'elles accèdent à ces données, ces autorités doivent respecter non seulement les règles mentionnées en B.16.8.2 à B.16.8.4, mais aussi les droits fondamentaux de l'utilisateur final, garantis notamment par le RGPD, par les articles 6 et 8 de la Convention européenne des droits de l'homme et par les articles 7, 8 et 47 de la Charte.

B.16.8.6. À cet égard, les parties requérantes renvoient à l'arrêt de la grande chambre de la Cour de justice du 2 mars 2021 en cause *Prokuratuur* (C-746/18, points 50 à 56), dans lequel la Cour de justice exige, selon elles, qu'une autorité administrative indépendante ou un juge contrôle au préalable chaque demande d'accès au regard des droits fondamentaux et règles nationales applicables et dans lequel elle précise, selon les parties requérantes, que le ministère public, qui dirige la procédure d'enquête et exerce le cas échéant l'action publique, ne dispose pas de l'indépendance requise pour pouvoir effectuer ce contrôle.

Toutefois, cet arrêt portait sur une demande du ministère public d'obtenir un accès à des données relatives au trafic et à des données de localisation. Comme il est dit en B.14.3, la Cour de justice et la Cour européenne des droits de l'homme n'exigent en revanche pas de contrôle judiciaire ou administratif préalable pour une demande d'accès à des données d'identification. En conséquence, le droit au respect de la vie privée ne s'oppose pas à une demande d'accès à de telles données qui émane du ministère public.

B.16.8.7. Cela étant, la demande d'accès aux données d'identification traitées en vertu de l'article 127 de la loi du 13 juin 2005 doit toujours être motivée *in concreto* par la démonstration du lien entre ces données et les éléments objectifs qui fondent la suspicion concrète initiale à l'égard de l'utilisateur final en question concernant une infraction spécifique. Il faut également motiver le fait que l'on ne demande pas davantage de données que celles qui sont strictement nécessaires dans le cadre de l'enquête en cours. Une telle motivation ne peut pas recourir à des formulations types ou à des formules de style.

B.16.9.1. La loi du 13 juin 2005 et les arrêtés royaux du 19 septembre 2013 et du 26 novembre 2016 contiennent des garanties contre les abus dans le cadre de la collecte, du traitement et de la conservation des données d'identification.

L'article 127, § 1er, de la loi du 13 juin 2005 dispose que le canal de vente de services de communications électroniques transmet les données d'identification et les documents d'identification collectés à l'opérateur, sans conserver lui-même de copies. Si l'introduction directe de ces données dans le système informatique n'est pas possible, le canal de vente peut faire une copie temporaire du document d'identification, qui doit être détruite au plus tard au moment de l'activation de la carte de téléphonie mobile prépayée.

En vertu de l'article 11, § 1er, de l'arrêté royal du 27 novembre 2016, l'entreprise concernée doit systématiquement vérifier si une carte d'identité présentée n'a pas été volée ou n'a pas fait l'objet d'une fraude. En vertu de l'article 12, alinéa 3, du même arrêté royal, l'entreprise concernée ou le fournisseur d'un service d'identification doit détruire la copie de la photo se trouvant sur la carte d'identité électronique au plus tard avant l'activation de la carte de téléphonie mobile prépayée.

En vertu de l'article 8 de l'arrêté royal du 19 septembre 2013, chaque fournisseur doit désigner parmi les membres de la Cellule de Coordination de Justice un préposé à la protection des données à caractère personnel, qui agit dans le cadre de la protection des données à caractère personnel en toute indépendance par rapport à ce fournisseur et qui a accès à toutes les données pertinentes ainsi qu'à tous les locaux pertinents de ce fournisseur. Il doit veiller à ce que tous les traitements poursuivent les objectifs mentionnés à l'article 126 de la loi du 13 juin 2005, que seules les personnes autorisées en vertu de cette disposition et de l'arrêté royal du

19 septembre 2013 aient accès aux données et que toutes les mesures de protection des données décrites à l'article 126 de la loi du 13 juin 2005 soient respectées.

B.16.9.2. En ce qui concerne l'accès aux données conservées, l'article 9 de l'arrêté royal du 19 septembre 2013 dispose que chaque fournisseur communique avant le 1er mars de chaque année à l'Institut belge des services postaux et des télécommunications le nombre de cas dans lesquels des données ont été, au cours de l'année civile écoulée, transmises aux autorités compétentes, le délai écoulé entre le traitement et la demande des données et les cas dans lesquels les demandes de données n'ont pas pu être satisfaites. Cet Institut transmet ces informations annuellement au ministre de la Justice.

En outre, en vertu de l'article 90*decies* du Code d'instruction criminelle, le ministre de la Justice fait rapport annuellement au Parlement sur l'application, notamment, des articles 46*bis*, 88*bis* et 90*ter* à 90*novies* du même Code. Cette communication concerne le nombre d'instructions ayant donné lieu aux mesures visées dans ces articles, la durée de ces mesures, le nombre de personnes concernées et les résultats obtenus.

En vertu de l'article 21 de la loi du 30 novembre 1998, les données à caractère personnel traitées dans le cadre de l'application de cette loi sont conservées par les services de renseignement et de sécurité pour une durée n'excédant pas celle qui est nécessaire aux finalités pour lesquelles elles sont enregistrées.

L'article 126, §§ 4 à 6, de la loi du 13 juin 2005, annulé par l'arrêt de la Cour n° 57/2021, prévoyait encore d'autres garanties contre les abus :

« § 4. Pour la conservation des données visées au paragraphe 3, les fournisseurs et les opérateurs visés au paragraphe 1er, alinéa 1er :

1° garantissent que les données conservées sont de la même qualité et sont soumises aux mêmes exigences de sécurité et de protection que les données sur le réseau;

2° veillent à ce que les données conservées fassent l'objet de mesures techniques et organisationnelles appropriées afin de les protéger contre la destruction accidentelle ou illicite, la perte ou l'altération accidentelle, ou le stockage, le traitement, l'accès ou la divulgation non autorisés ou illicites;

3° garantissent que l'accès aux données conservées pour répondre aux demandes des autorités visées au paragraphe 2 n'est effectué que par un ou plusieurs membres de la Cellule de coordination visée à l'article 126/1, § 1er;

4° conservent les données sur le territoire de l'Union européenne;

5° mettent en œuvre des mesures de protection technologique qui rendent les données conservées, dès leur enregistrement, illisibles et inutilisables par toute personne qui n'est pas autorisée à y avoir accès;

6° détruisent les données conservées de tout support lorsqu'est expiré le délai de conservation applicable à ces données fixé au paragraphe 3, sans préjudice des articles 122 et 123;

7° assurent une traçabilité de l'exploitation des données conservées pour chaque demande d'obtention de ces données d'une autorité visée au paragraphe 2.

La traçabilité visée à l'alinéa 1er, 7°, s'effectue à l'aide d'un journal. L'Institut et la Commission pour la protection de la vie privée peuvent consulter ce journal ou exiger une copie de tout ou partie de ce journal. L'Institut et la Commission pour la protection de la vie privée concluent un protocole de collaboration concernant la prise de connaissance et le contrôle du contenu du journal.

§ 5. Le ministre et le ministre de la Justice font en sorte que des statistiques sur la conservation des données qui sont générées ou traitées dans le cadre de la fourniture de services ou réseaux de communications accessibles au public soient transmises annuellement à la Chambre des représentants.

Ces statistiques comprennent notamment :

1° les cas dans lesquels des données ont été transmises aux autorités compétentes conformément aux dispositions légales applicables;

2° le laps de temps écoulé entre la date à partir de laquelle les données ont été conservées et la date à laquelle les autorités compétentes ont demandé leur transmission;

3° les cas dans lesquels des demandes de données n'ont pu être satisfaites.

Ces statistiques ne peuvent comprendre des données à caractère personnel.

Les données qui concernent l'application du paragraphe 2, 1°, sont également jointes au rapport que le ministre de la Justice doit faire au Parlement conformément à l'article 90*decies* du Code d'instruction criminelle.

Le Roi détermine, sur proposition du ministre de la Justice et du ministre et sur avis de l'Institut, les statistiques que les fournisseurs et opérateurs visés au paragraphe 1er, alinéa 1er, transmettent annuellement à l'Institut et celles que l'Institut transmet au ministre et au ministre de la Justice.

§ 6. Sans préjudice du rapport visé au paragraphe 5, alinéa 4, le ministre et le ministre de la Justice font un rapport d'évaluation à la Chambre des représentants, deux ans après l'entrée en vigueur de l'arrêté royal visé au paragraphe 3, alinéa 4, sur la mise en œuvre du présent article, afin de vérifier si des dispositions doivent être adaptées, en particulier en ce qui concerne les données à conserver et la durée de la conservation ».

Il appartient au législateur, lorsqu'il créera un nouveau cadre législatif en matière de conservation des données répondant aux critères mentionnés dans l'arrêt n° 57/2021, d'y inclure à nouveau des garanties contre les abus. En attendant qu'il le fasse – et compte tenu des autres garanties contre les abus qui sont mentionnées –, l'absence d'une telle disposition, qui porte uniquement sur l'accès aux données personnelles conservées, ne peut pas conduire à l'annulation de la loi attaquée, qui traite en effet uniquement de la collecte, du traitement et de la conservation initiaux des données d'identification des utilisateurs d'une carte de téléphonie mobile prépayée.

B.16.10. L'article 127 de la loi du 13 juin 2005 ne prévoit pas de contrôle juridictionnel spécifique du traitement des données d'identification traitées en vertu de l'article 127 de la loi du 13 juin 2005. Toutefois, comme il est dit en B.14.3, les recours de droit commun suffisent en matière de traitement de simples données d'identification et d'accès à celles-ci (CEDH, 30 janvier 2020, *Breyer c. Allemagne*, § 106).

Dans le cadre de la procédure pénale, le prévenu dispose à cet égard du droit d'invoquer devant les juridictions d'instruction ou devant la juridiction de jugement la nullité d'un acte d'instruction qui viole son droit au respect de la vie privée ou son droit à un procès équitable.

Dans le cadre du fonctionnement des services de renseignement et de sécurité, l'intéressé dispose, en vertu de l'article 79 de la loi du 30 juillet 2018 « relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel », du droit de demander au Comité permanent R de faire rectifier ou supprimer ses données à caractère personnel inexactes et de vérifier le respect des dispositions applicables.

De plus, chaque utilisateur final d'une carte de téléphonie mobile prépayée dont les données d'identification ont été traitées en violation de l'article 127 de la loi du 13 juin 2005 et de l'arrêté royal du 27 novembre 2016 dispose d'une action en responsabilité de droit commun contre la personne qui a enfreint cette disposition législative.

Enfin, l'intéressé peut, en vertu de l'article 58 de la loi du 3 décembre 2017 « portant création de l'Autorité de protection des données », déposer sans frais une plainte auprès de l'Autorité de protection des données en cas de traitement illégitime de ses données à caractère personnel.

B.16.11.1. Les trois objectifs légitimes que le législateur poursuit avec l'article 127 de la loi du 13 juin 2005, à savoir le bon fonctionnement des services d'urgence, la détection, la poursuite et la répression d'infractions et la collecte d'informations par les services de renseignement et de sécurité, sont tous liés aux obligations positives qui incombent aux autorités publiques en matière de droit à la vie, d'interdiction de traitements inhumains et dégradants et de droit à la liberté et à la sécurité de toute la population.

B.16.11.2. Une mesure qui prévoit l'identifiabilité de tous les utilisateurs finaux d'une carte de téléphonie mobile prépayée est pertinente pour atteindre ces objectifs.

La possibilité de céder une carte de téléphonie mobile prépayée et la possibilité qu'elle soit volée ne suffisent pas pour arriver à une autre conclusion. C'est d'ailleurs la raison pour laquelle l'article 127, § 1er, alinéa 3, de la loi du 13 juin 2005 dispose que la personne identifiée est réputée utiliser elle-même le service de communications électroniques. Cette disposition vise à l'inciter à la prudence en ce qui concerne l'utilisation de sa carte de téléphonie mobile prépayée par des tiers. L'article 5 de l'arrêté royal du 27 novembre 2016 limite en outre la possibilité de céder une carte de téléphonie mobile prépayée à des tiers : sauf dans l'hypothèse où la carte de téléphonie mobile est cédée à un proche de la famille (article 5, 1° à 3°), une cession n'est possible que si ce tiers s'identifie au préalable auprès de l'entreprise concernée (article 5, 4°), si une personne morale qui attribue une carte de téléphonie mobile à une personne physique effectuant des prestations pour elle conserve une liste actualisée des personnes à qui elle a donné une carte (article 5, 5°), ou si la carte de téléphonie mobile est achetée pour le compte des services de renseignement et de sécurité, des services de police ou de certaines autorités désignées par arrêté royal (article 5, 6°). En cas de perte ou de vol de la carte de téléphonie mobile, l'article 6 du même arrêté royal oblige l'utilisateur final à en informer l'entreprise concernée dans les 24 heures.

De même, l'existence d'autres techniques de communication n'empêche pas le législateur de supprimer l'anonymat des cartes de téléphonie mobile prépayées s'il constate notamment que ces cartes de téléphonie mobile sont utilisées dans des milieux terroristes et criminels et que cet anonymat constitue un problème insurmontable pour les autorités judiciaires et pour les services de renseignement et de sécurité. Au demeurant, si la disposition attaquée a pour effet que les organisations terroristes et criminelles passent à des techniques plus avancées, cela démontre plutôt la pertinence de la mesure attaquée. Il appartient alors au législateur de réguler également l'utilisation de ces techniques, en vue de réaliser les mêmes objectifs.

B.16.11.3. Compte tenu des garanties mentionnées en B.16.1 à B.16.9.3, l'identifiabilité de l'utilisateur final d'une carte de téléphonie mobile prépayée, qui doit être considérée comme une mesure présentant une faible incidence sur la vie privée, est également proportionnée au regard de ces objectifs. Le fait que cette mesure porte sur tous les utilisateurs finaux de carte de téléphonie mobile prépayée, même s'ils ne sauraient être suspectés du moindre comportement criminel, n'y change rien, étant donné qu'une mesure d'identifiabilité ne peut fonctionner que pour autant que toute personne puisse être identifiée dès que nécessaire.

B.16.11.4. Enfin, les utilisateurs de cartes de téléphonie mobile prépayées ne pouvaient pas ignorer le fait que l'anonymat de ces cartes de téléphonie mobile serait un jour supprimé. Comme il est dit en B.2.1 à B.2.7, cet anonymat a en effet toujours été conçu comme une exception temporaire à la règle selon laquelle tous les utilisateurs finaux de réseaux de communications électroniques doivent être identifiables.

B.16.12. Sous réserve des interprétations mentionnées en B.8.7.3, B.16.6, B.16.8.5 et B.16.8.7, le deuxième moyen, en sa première branche, n'est pas fondé.

En ce qui concerne la deuxième branche du deuxième moyen

B.17. Dans la deuxième branche du deuxième moyen, les parties requérantes font valoir que la loi attaquée viole la liberté d'établissement et la libre prestation des services.

B.18. Toute mesure nationale qui peut avoir pour effet de gêner ou de rendre moins attrayante la libre prestation des services par des entreprises d'un autre État membre de l'Union

européenne constitue une restriction de la libre prestation de services. Par ailleurs, l'article 56 du Traité sur le fonctionnement de l'Union européenne accorde des droits non seulement au prestataire des services, mais aussi au destinataire de ceux-ci.

Une telle restriction peut toutefois être justifiée par des « raisons impérieuses d'intérêt général, à condition qu'elles soient propres à garantir la réalisation de l'objectif poursuivi et qu'elles n'aillent pas au-delà de ce qui est nécessaire pour atteindre cet objectif, à savoir s'il n'existe pas des mesures moins restrictives qui permettraient de l'atteindre de manière aussi efficace » (CJUE, 11 février 2021, C-407/19 et C-471/19, *Katoen Natie Bulk Terminals NV e.a.*, points 59 à 61).

B.19.1. Sans qu'il soit nécessaire d'examiner si la loi attaquée restreint la liberté d'établissement ou la libre prestation de services, il suffit de constater qu'elle est justifiée par des raisons impérieuses d'intérêt général, à savoir le bon fonctionnement des services d'urgence, la détection, la poursuite et la répression efficaces d'infractions pénales et la prévention d'activités terroristes, en assurant que les services de renseignement et de sécurité puissent associer des menaces éventuelles à l'identité de personnes dont des communications ont été interceptées.

B.19.2. Comme il est dit en B.16.11.2, la loi attaquée est pertinente eu égard à ces objectifs. De plus, elle ne va pas au-delà de ce qui est nécessaire pour les atteindre. Une mesure qui vise à assurer que les utilisateurs finaux d'un réseau de communications électroniques belge soient identifiables ne peut en effet être utile que si elle est applicable sans exception à tous les utilisateurs finaux de ce réseau, indépendamment du fait qu'ils téléphonent au moyen d'un abonnement ou d'une carte de téléphonie mobile prépayée, que cette carte ait déjà été achetée avant l'entrée en vigueur de la loi attaquée ou non et qu'il s'agisse d'une carte de téléphonie fournie par une entreprise établie en Belgique ou dans un autre État membre de l'Union européenne.

L'exclusion des cartes de téléphonie mobile prépayées fournies par des entreprises établies dans un autre État membre du champ d'application de l'article 127 de la loi du 13 juin 2005 rendrait l'identifiabilité impossible dans la pratique, étant donné, notamment, que des personnes mal intentionnées pourraient aisément s'y soustraire en achetant une carte de téléphonie mobile prépayée d'une entreprise établie dans un autre État membre.

B.19.3. Le deuxième moyen, en sa deuxième branche, n'est pas fondé.

En ce qui concerne la troisième branche du deuxième moyen

B.20. Dans la troisième branche du deuxième moyen, les parties requérantes font valoir que la loi attaquée viole la liberté d'expression, étant donné que l'identifiabilité des utilisateurs finaux d'une carte de téléphonie mobile prépayée les dissuaderait d'informer des personnalités politiques et des journalistes et limiterait ainsi de manière disproportionnée la liberté de recevoir des informations et des idées ainsi que le secret des sources des journalistes.

B.21.1. La liberté d'expression constitue l'un des fondements essentiels d'une société démocratique. Elle vaut non seulement pour les « informations » ou « idées » accueillies avec faveur ou considérées comme inoffensives ou indifférentes, mais aussi pour celles qui « choquent, inquiètent ou heurtent » l'État ou une fraction de la population. Ainsi le veulent le pluralisme, la tolérance et l'esprit d'ouverture sans lesquels il n'est pas de société démocratique (CEDH, 7 décembre 1976, *Handyside c. Royaume-Uni*, § 49; 23 septembre 1998, *Lehideux et Isorni c. France*, § 55; 28 septembre 1999, *Öztürk c. Turquie*, § 64; grande chambre, 13 juillet 2012, *Mouvement Raëlien suisse c. Suisse*, § 48).

Ainsi qu'il ressort des termes de l'article 10, paragraphe 2, de la Convention européenne des droits de l'homme, l'exercice de la liberté d'expression implique néanmoins certaines obligations et responsabilités (CEDH, 4 décembre 2003, *Gündüz c. Turquie*, § 37), notamment le devoir de principe de ne pas franchir certaines limites « tenant notamment à la protection de la réputation et aux droits d'autrui » (CEDH, 24 février 1997, *De Haes et Gijsels c. Belgique*, § 37; 21 janvier 1999, *Fressoz et Roire c. France*, § 45; 15 juillet 2003, *Ernst e.a. c. Belgique*, § 92). La liberté d'expression peut, en vertu de l'article 10, paragraphe 2, de la Convention européenne des droits de l'homme, être soumise, sous certaines conditions, à certaines formalités, conditions, restrictions ou sanctions, en vue, notamment, de la protection de la réputation ou des droits d'autrui. Les exceptions dont il est assorti appellent toutefois « une

interprétation étroite, et le besoin de la restreindre doit se trouver établi de manière convaincante » (CEDH, grande chambre, 20 octobre 2015, *Pentikäinen c. Finlande*, § 87).

L'article 19 de la Constitution interdit que la liberté d'expression soit soumise à des restrictions préventives, mais non que les infractions qui sont commises à l'occasion de la mise en œuvre de cette liberté soient sanctionnées.

B.21.2. Le droit au secret des sources journalistiques doit être garanti, non pas pour protéger les intérêts des journalistes en tant que groupe professionnel, mais bien pour permettre à la presse de jouer son rôle de « chien de garde » et d'informer le public sur des questions d'intérêt général. Pour ces motifs, ce droit fait partie de la liberté d'expression et de la liberté de la presse.

B.21.3. Selon la Cour de justice, « une transmission des données relatives au trafic et des données de localisation à des autorités publiques à des fins sécuritaires est susceptible […] d'entraîner des effets dissuasifs sur l'exercice par les utilisateurs […] de leur liberté d'expression, garantie à l'article 11 de la Charte. De tels effets dissuasifs peuvent affecter en particulier les personnes dont les communications sont soumises, selon les règles nationales, au secret professionnel ainsi que les lanceurs d'alertes dont les activités sont protégées par la directive (UE) 2019/1937 du Parlement européen et du Conseil, du 23 octobre 2019, sur la protection des personnes qui signalent des violations du droit de l'Union (*JO*, 2019, L-305, p. 17). En outre, ces effets sont d'autant plus graves que le nombre et la variété des données conservées sont élevés » (CJUE, grande chambre, 6 octobre 2020, C-623/17, *Privacy international*, point 72; voir dans le même sens CJUE, grande chambre, 8 avril 2014, C-293/12 et C-594/12, *Digital Rights Ireland e.a.*, point 28; 21 décembre 2016, C-203/15 et C-698/15, *Tele2 Sverige e.a.*, point 101; 6 octobre 2020, C-511/18, C-512/18 et C-520/18, *La Quadrature du Net e.a.*, point 118).

B.22. L'article 127 de la loi du 13 juin 2005 porte uniquement sur la conservation et le traitement des données d'identification visées à l'article 12 de l'arrêté royal du 27 novembre 2016. À elles seules, ces données ne donnent pas d'information sur les opinions personnelles de la personne identifiée. De même, les données relatives au trafic et les données de localisation auxquelles elles pourraient être associées ne constituent pas en soi l'expression d'une opinion.

Ce n'est que si ces données étaient également liées au contenu d'une communication effectuée et que l'analyse de celles-ci entraînait d'autres mesures, telles qu'une enquête par les services de renseignement et de sécurité ou une instruction pénale, qu'il pourrait en résulter une limitation de la liberté d'expression, de la liberté d'obtenir des informations, de la liberté de presse ou du secret des sources.

Comme il est dit en B.15.3, une association des données d'identification à d'autres métadonnées ou au contenu d'une communication doit toutefois être fondée sur une disposition législative claire et sans équivoque, respecter les conditions matérielles et procédurales de cette disposition et être compatible avec les droits fondamentaux de l'intéressé.

Un tel lien indirect entre la suppression, attaquée, de l'anonymat des cartes de téléphonie mobile prépayées et le contenu des communications effectuées ne suffit pas pour considérer que la loi attaquée limite la liberté d'expression. La simple collecte de données d'identification de tous les utilisateurs finaux d'un réseau de communications électroniques ne saurait justifier la crainte, dans un État de droit démocratique, que toutes les communications menées sur ce réseau seront supervisées par les pouvoirs publics. La loi attaquée ne saurait dès lors avoir pour effet, par elle-même, de dissuader des personnes d'exprimer leur opinion ou de partager des informations avec des journalistes ou avec des personnalités politiques.

Le deuxième moyen, en sa troisième branche, n'est pas fondé.

Quant au troisième moyen

B.23. Les parties requérantes prennent un troisième moyen de la violation, par l'article 2, 1°, c), de la loi attaquée, des articles 10, 11, 12 et 14 de la Constitution, lus en combinaison avec les articles 6 et 7 de la Convention européenne des droits de l'homme, avec les articles 48, 49 et 52 de la Charte, avec le droit à un procès équitable, avec la présomption d'innocence et avec le principe de légalité en matière pénale, en ce que la présomption, contenue dans cette disposition, d'imputabilité de la communication à l'utilisateur final de la carte de téléphonie mobile prépayée qui a été identifié peut avoir pour effet de rendre cette personne responsable de faits qu'elle n'a pas commis.

B.24.1. L’article 12 de la Constitution dispose :

« La liberté individuelle est garantie.

Nul ne peut être poursuivi que dans les cas prévus par la loi, et dans la forme qu’elle prescrit.

Hors le cas de flagrant délit, nul ne peut être arrêté qu’en vertu d’une ordonnance motivée du juge qui doit être signifiée au plus tard dans les quarante-huit heures de la privation de liberté et ne peut emporter qu’une mise en détention préventive ».

L’article 14 de la Constitution dispose :

« Nulle peine ne peut être établie ni appliquée qu’en vertu de la loi ».

L’article 7 de la Convention européenne des droits de l’homme dispose :

« 1. Nul ne peut être condamné pour une action ou une omission qui, au moment où elle a été commise, ne constituait pas une infraction d’après le droit national ou international. De même il n’est infligé aucune peine plus forte que celle qui était applicable au moment où l’infraction a été commise.

2. Le présent article ne portera pas atteinte au jugement et à la punition d’une personne coupable d’une action ou d’une omission qui, au moment où elle a été commise, était criminelle d’après les principes généraux de droit reconnus par les nations civilisées ».

L’article 49 de la Charte dispose :

« 1. Nul ne peut être condamné pour une action ou une omission qui, au moment où elle a été commise, ne constituait pas une infraction d’après le droit national ou le droit international. De même, il n’est infligé aucune peine plus forte que celle qui était applicable au moment où l’infraction a été commise. Si, postérieurement à cette infraction, la loi prévoit une peine plus légère, celle-ci doit être appliquée.

2. Le présent article ne porte pas atteinte au jugement et à la punition d’une personne coupable d’une action ou d’une omission qui, au moment où elle a été commise, était criminelle d’après les principes généraux reconnus par l’ensemble des nations.

3. L’intensité des peines ne doit pas être disproportionnée par rapport à l’infraction ».

B.24.2. En attribuant au pouvoir législatif la compétence pour déterminer dans quels cas des poursuites pénales sont possibles, l’article 12, alinéa 2, de la Constitution garantit à tout

justiciable qu'aucun comportement ne sera punissable qu'en vertu de règles adoptées par une assemblée délibérante, démocratiquement élue.

En outre, le principe de légalité en matière pénale qui découle de la disposition constitutionnelle précitée procède de l'idée que la loi pénale doit être formulée en des termes qui permettent à chacun de savoir, au moment où il adopte un comportement, si celui-ci est ou non punissable. Il exige que le législateur indique, en des termes suffisamment précis, clairs et offrant la sécurité juridique, quels faits sont sanctionnés, afin, d'une part, que celui qui adopte un comportement puisse évaluer préalablement, de manière satisfaisante, quelle sera la conséquence pénale de ce comportement et afin, d'autre part, que ne soit pas laissé au juge un trop grand pouvoir d'appréciation.

Toutefois, le principe de légalité en matière pénale n'empêche pas que la loi attribue un pouvoir d'appréciation au juge. Il faut en effet tenir compte du caractère de généralité des lois, de la diversité des situations auxquelles elles s'appliquent et de l'évolution des comportements qu'elles répriment.

La condition qu'une infraction doit être clairement définie par la loi se trouve remplie lorsque le justiciable peut savoir, à partir du libellé de la disposition pertinente et, au besoin, à l'aide de son interprétation par les juridictions, quels actes et omissions engagent sa responsabilité pénale.

Ce n'est qu'en examinant une disposition pénale spécifique qu'il est possible de déterminer, en tenant compte des éléments propres aux infractions qu'elle entend réprimer, si les termes généraux utilisés par le législateur sont à ce point vagues qu'ils méconnaîtraient le principe de légalité en matière pénale.

B.24.3. La disposition attaquée n'incrimine aucun comportement et ne définit pas de peines pour des infractions spécifiques. Contrairement à ce que les parties requérantes font valoir, elle n'impute pas non plus automatiquement à l'utilisateur final d'une carte de téléphonie mobile prépayée qui a été identifié les infractions qui sont découvertes ou prouvées à la suite de l'analyse de l'utilisation de cette carte de téléphonie mobile.

L'article 127, § 1er, alinéa 3, de la loi du 13 juin 2005 contient seulement la présomption réfragable selon laquelle cet utilisateur final est également celui qui utilise cette carte de téléphonie mobile. Le principe de légalité en matière pénale n'est pas applicable à une telle disposition.

B.25. L'article 6, paragraphe 2, de la Convention européenne des droits de l'homme dispose :

« Toute personne accusée d'une infraction est présumée innocente jusqu'à ce que sa culpabilité ait été légalement établie ».

L'article 48, paragraphe 1, de la Charte dispose :

« Tout accusé est présumé innocent jusqu'à ce que sa culpabilité ait été légalement établie ».

Conformément à ces dispositions, toute personne accusée d'une infraction est présumée innocente jusqu'à ce que sa culpabilité ait été légalement établie.

Les présomptions légales ne sont en principe pas contraires à la présomption d'innocence (voir en ce sens : CEDH, 7 octobre 1988, *Salabiaku c. France*, § 28; 20 mars 2001, *Telfner c. Autriche*, § 16). Elles doivent toutefois être raisonnablement proportionnées au but légitime poursuivi (CEDH, 23 juillet 2002, *Janosevic c. Suède*, § 101; 23 juillet 2002, *Västberga Taxi Aktiebolag et Vulic c. Suède*, § 113), en prenant en compte la gravité de l'enjeu et en préservant les droits de la défense (CEDH, 4 octobre 2007, *Anghel c. Roumanie*, § 60).

B.26.1. À l'origine, l'avant-projet qui a donné lieu à la loi attaquée disposait que la personne identifiée était « responsable » de l'utilisation du service de communications électroniques qui lui était fourni. Dans l'avis n° 59.423/4 du 15 juin 2016, la section de législation du Conseil d'État a formulé l'observation suivante à ce sujet :

« À l'article 127, § 1er, alinéa 3, en projet, la section de législation n'aperçoit pas quelle est la portée concrète de la règle en projet, à savoir celle qui prévoit que la personne physique ou morale identifiée est ' responsable ' de l'utilisation du service de communications électroniques qui lui est fourni : quelle est la responsabilité ainsi visée ? S'agit-il de la responsabilité contractuelle à l'égard de l'opérateur, d'une responsabilité aquilienne à l'égard de tiers, ou encore d'une responsabilité pénale ?

Le texte en projet sera revu afin de préciser expressément quelle est la teneur et la portée de la responsabilité envisagée, spécialement si une quelconque responsabilité pénale est ainsi couverte » (*Doc. parl.*, Chambre, 2015-2016, DOC 54-1964/001, pp. 46-47).

Compte tenu de cet avis, le législateur a supprimé du projet toute référence à la « responsabilité » de l'utilisateur final. Lors des travaux préparatoires, la version finale de la disposition attaquée a été commentée comme suit :

« Le nouvel alinéa introduit a été revu en profondeur suite à l'avis du Conseil d'État qui estimait qu'il n'apercevait pas la portée concrète de la règle en projet.

Le principe selon lequel la personne identifiée est en principe l'utilisateur effectif du service de communications électroniques (sauf preuve contraire) permet d'éviter qu'une personne s'identifie à la place d'un tiers qui utilise effectivement le service de communications électroniques pour cacher l'identité de ce tiers » (*ibid.*, p. 9).

B.26.2. La disposition attaquée n'établit dès lors pas de responsabilité pénale automatique ou de responsabilité objective de l'utilisateur final d'une carte de téléphonie mobile prépayée qui a été identifié en ce qui concerne l'utilisation qu'en fait un tiers. Elle remplit principalement une fonction d'avertissement, étant donné qu'elle rappelle la présomption de départ de toute enquête pénale et de toute enquête par les services de renseignement et de sécurité, à savoir la présomption selon laquelle c'est le propriétaire ou l'utilisateur habituel d'un objet qui l'a utilisé pour commettre l'infraction ou pour menacer la sécurité nationale. Les enquêteurs écartent cette présomption dès qu'elle est infirmée par les éléments de preuve recueillis.

Par ailleurs, il convient de lire la disposition attaquée, comme il est dit en B.16.11.2, en combinaison avec les articles 5 et 6 de l'arrêté royal du 27 novembre 2016, qui limitent la possibilité de céder la carte de téléphonie mobile prépayée et qui obligent l'utilisateur final à signaler à l'opérateur la perte ou le vol de cette carte dans les 24 heures. L'ensemble de ces dispositions contribue à la pertinence de l'article 127 de la loi du 13 juin 2005, puisque le but est de faciliter l'identifiabilité du véritable utilisateur d'une carte de téléphonie mobile prépayée.

B.26.3. La disposition attaquée est donc en rapport avec les objectifs que poursuit le législateur par l'article 127 de la loi du 13 juin 2005, à savoir ceux qui portent sur des situations et des enquêtes urgentes.

B.26.4. En outre, la disposition attaquée est souvent appliquée dans le cadre d'infractions ou de menaces pour la sécurité nationale susceptibles d'avoir des conséquences graves sur l'intégrité physique de personnes ou de causer des troubles sociétaux considérables.

B.26.5. L'utilisateur final identifié dispose de plusieurs possibilités pour se défendre dans le cadre des poursuites pénales qui pourraient découler de l'utilisation de sa carte de téléphonie mobile prépayée faite par un tiers. S'il informe les enquêteurs de la personne qui a utilisé sa carte de téléphonie mobile prépayée, ceux-ci doivent examiner l'implication de cette personne.

Du reste, la disposition attaquée se contente d'instaurer une présomption réfragable, que le prévenu peut contester par toutes voies de droit. Elle ne lui interdit pas de présenter tous les éléments de fait qui infirment son implication dans les infractions commises ou dans les menaces pour la sécurité nationale qui font l'objet d'une enquête.

Par ailleurs, la disposition attaquée n'enlève rien au principe selon lequel il revient au ministère public, dans un procès pénal, de prouver la culpabilité du prévenu. Il appartient au juge répressif d'apprécier la valeur probante de tous les éléments de preuve, en ce compris les explications du prévenu, en respectant son droit à un procès équitable.

La disposition attaquée ne portant donc pas atteinte aux droits de défense du prévenu, elle ne compromet pas non plus la présomption d'innocence.

B.26.6. Contrairement à ce que les parties requérantes font valoir, ce qui précède vaut tout autant pour l'implication de l'utilisateur final identifié dans les infractions terroristes mentionnées aux articles 137 à 141*ter* du Code pénal. Il ne peut être condamné en tant que coauteur ou complice de telles infractions que si le ministère public démontre à son encontre que tous les éléments constitutifs de ces infractions, y compris l'élément intentionnel, sont réunis en ce qui le concerne.

La mise à disposition de bonne foi d'une carte de téléphonie mobile prépayée par un utilisateur final qui ne pouvait pas présumer qu'elle serait utilisée pour commettre ou pour préparer une telle infraction ne saurait justifier en soi une condamnation pénale.

B.26.7. Sous réserve des interprétations mentionnées en B.26.2 et B.26.6, le troisième moyen n'est pas fondé.

Quant au quatrième moyen

B.27.1. Les parties requérantes prennent un quatrième moyen de la violation, par l'article 3 de la loi attaquée, des articles 10, 11 et 22 de la Constitution, lus en combinaison avec l'article 8 de la Convention européenne des droits de l'homme, avec les articles 7, 8 et 52 de la Charte, avec les articles 2, point a), 6, 13 et 22 de la directive 95/46/CE et avec les articles 1er, 2, 3, 5, 6, 9 et 15 de la directive 2002/58/CE . Ce moyen est subdivisé en cinq branches.

B.27.2. Dans la première branche, les parties requérantes font valoir que la disposition attaquée donne aux services de renseignement et de sécurité un accès aux données d'identification collectées sur la base de l'article 127 de la loi du 13 juin 2005, sans limiter cet accès aux infractions graves.

Dans la deuxième branche, elles soutiennent que cet accès des services de renseignement et de sécurité n'est pas soumis à un contrôle préalable effectué par une juridiction ou par une autorité administrative indépendante.

Dans la troisième branche, elles reprochent à la disposition attaquée de ne pas préciser suffisamment les conditions matérielles et procédurales de cet accès.

Dans la quatrième branche, elles déplorent le fait que la disposition attaquée n'oblige pas les services de renseignement et de sécurité qui ont accès aux données d'identification traitées en vertu de l'article 127 de la loi du 13 juin 2005 à en informer l'intéressé, de sorte qu'il puisse exercer son droit à un contrôle juridictionnel effectif.

Dans la cinquième branche, les parties requérantes font valoir que la disposition attaquée n'exclut pas que des services de renseignement et de sécurité étrangers aient accès à ces données.

Eu égard à leur connexité, ces branches doivent être traitées conjointement.

B.28.1. En vertu de l'article 1er, paragraphe 3, de la directive 2002/58/CE, cette dernière « ne s'applique pas aux activités qui ne relèvent pas du traité instituant la Communauté européenne, telles que celles visées dans les titres V et VI du traité sur l'Union européenne et, en tout état de cause, aux activités concernant la sécurité publique, la défense, la sûreté de l'État (y compris la prospérité économique de l'État lorsqu'il s'agit d'activités liées à la sûreté de l'État) ou aux activités de l'État dans des domaines relevant du droit pénal ».

En vertu de l'article 2, paragraphe 2, point a), du RGPD, ce règlement « ne s'applique pas au traitement de données à caractère personnel effectué dans le cadre d'une activité qui ne relève pas du champ d'application du droit de l'Union ». En vertu de l'article 2, paragraphe 2, point d), du RGPD, il ne s'applique pas non plus au traitement des données à caractère personnel effectué par les autorités compétentes à des fins de protection et de prévention des menaces pour la sécurité publique.

Par son arrêt du 6 octobre 2020 en cause *La Quadrature du Net e.a.* (C-511/18, C-512/18 et C-520/18), la grande chambre de la Cour de justice a jugé :

« 135. À cet égard, il convient de relever, d'emblée, que l'article 4, paragraphe 2, TUE énonce que la sécurité nationale reste de la seule responsabilité de chaque État membre. Cette responsabilité correspond à l'intérêt primordial de protéger les fonctions essentielles de l'État et les intérêts fondamentaux de la société et inclut la prévention et la répression d'activités de nature à déstabiliser gravement les structures constitutionnelles, politiques, économiques ou sociales fondamentales d'un pays, et en particulier à menacer directement la société, la population ou l'État en tant que tel, telles que notamment des activités de terrorisme ».

B.28.2. La disposition attaquée insère dans la loi du 30 novembre 1998 un nouvel article 16/2, § 2. En vertu de cette disposition, les services de renseignement et de sécurité peuvent, dans l'intérêt de l'exercice de leurs missions, requérir le concours d'une banque ou d'une institution financière pour procéder à l'identification de l'utilisateur final d'une carte de

téléphonie mobile prépayée sur la base de la référence d'une transaction bancaire électronique qui est liée à cette carte de téléphonie mobile et qui a préalablement été communiquée par l'entreprise concernée.

B.28.3. Étant donné que la disposition attaquée n'est applicable que dans le cadre des missions des services de renseignement et de sécurité, elle ne relève pas du champ d'application du droit de l'Union européenne. Le moyen est dès lors irrecevable en ce qu'il est pris de la violation des dispositions invoquées de la Charte, du RGPD ou de la directive 2002/58/CE.

B.29.1. L'accès d'une autorité aux données bancaires relève du champ d'application du droit au respect de la vie privée, indépendamment du fait que ces données soient sensibles ou non ou qu'elles aient un rapport ou non avec l'exercice de la profession (CEDH, 7 juillet 2005, *M.N. e.a. c. Saint-Marin*, §§ 51-55; 1er décembre 2015, *Brito Ferrinho Bexiga Villa-Nova c. Portugal*, § 44; 27 avril 2017, *Sommer c. Allemagne*, § 48).

B.29.2. L'accès de l'autorité publique aux données bancaires doit être basé sur une habilitation légale spécifique qui en délimite clairement et sans équivoque l'objet ainsi que le seuil pour y accéder. Cet objet doit être limité à ce qui est nécessaire au regard de l'objectif légitime poursuivi, étant donné qu'un accès trop large aux données bancaires permettrait à l'autorité publique de se faire une idée détaillée de la vie privée de l'intéressé. L'autorité publique ne peut avoir accès à de telles données que si elle dispose d'indices concrets que le titulaire du compte bancaire est impliqué dans une infraction. La loi doit également prévoir des mesures contre les abus, parmi lesquelles la garantie que les données ne seront pas conservées plus longtemps que ce qui est nécessaire aux fins de l'investigation menée. Enfin, il doit exister un contrôle juridictionnel effectif du respect de ces garanties matérielles et procédurales (CEDH, 27 avril 2017, *Sommer c. Allemagne*, §§ 57-63).

B.30.1. La disposition attaquée précise les services qui disposent de l'habilitation visée en B.28.2 et les institutions qui sont tenues d'apporter leur concours.

Elle délimite également de deux manières l'objectif de la mesure attaquée. Premièrement, elle vise à identifier soit l'utilisateur final d'une carte de téléphonie mobile prépayée visé à l'article 127 de la loi du 13 juin 2005, soit la carte de téléphonie mobile prépayée qui est utilisée

par une certaine personne. Deuxièmement, cette identification doit s'inscrire dans le cadre des missions des services de renseignement et de sécurité.

B.30.2. L'objet de l'acte d'investigation est limité à une transaction bancaire spécifique, à savoir celle qui a permis d'acheter une carte de téléphonie mobile prépayée. Un tel acte d'investigation ne permet aux services de renseignement et de sécurité que de recueillir des données d'identification, mais ne leur fournit pas à lui seul des données relatives au trafic ou des données de localisation, ni un accès aux communications effectuées.

La disposition attaquée ne leur permet pas non plus d'obtenir, par ce seul acte d'investigation, d'autres informations financières relatives au titulaire du compte bancaire. Elle ne leur permet donc pas, à l'aide des seules données d'identification obtenues, de se faire une idée de ses habitudes de dépenses faites par le titulaire du compte bancaire ou de toute autre information personnelle sensible le concernant.

Comme il est dit en B.15.3, s'il est vrai que ces données d'identification peuvent ensuite être associées à d'autres données et que la disposition attaquée peut ainsi contribuer à la divulgation de telles informations sensibles, ces informations doivent alors être recueillies à l'aide d'autres actes d'investigation, qui doivent à leur tour respecter la législation applicable et les droits fondamentaux de l'intéressé.

B.30.3. Comme il est dit en B.3.3, l'identification sur la base de la disposition attaquée peut s'avérer nécessaire en fonction de la méthode d'identification que l'utilisateur final a choisie lors de l'achat de la carte de téléphonie mobile prépayée.

Si, lors de l'achat de la carte de téléphonie mobile prépayée, il opte pour l'identification sur la base de l'opération de paiement en ligne, les services de renseignement et de sécurité ne peuvent l'identifier que s'ils disposent de la référence de la transaction bancaire électronique et qu'ils peuvent l'associer tant à la carte de téléphonie mobile qu'à l'identité de l'utilisateur final (*Doc. parl.*, Chambre, 2015-2016, DOC 54-1964/001, pp. 14-16). Cette méthode d'identification est réglée à l'article 17 de l'arrêté royal du 27 novembre 2016, qui dispose :

« § 1er. L'entreprise concernée peut identifier l'utilisateur final sur la base d'une opération de paiement électronique en ligne spécifique à l'achat ou la recharge de la carte prépayée.

Cette méthode est soumise aux conditions suivantes :

1° l'opération de paiement doit être traitée par un prestataire de services de paiement tel que visé à l'art. I.9. 2°, a), b), c), et d) du Code de droit économique;

2° Le prestataire de services de paiement est soumis à la loi du 11 janvier 1993 relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux et du financement du terrorisme;

3° une nouvelle identification doit être effectuée dans les 18 mois qui suivent l'opération de paiement liée à la carte prépayée;

4° l'utilisateur final introduit sur un formulaire en ligne de l'entreprise concernée au minimum son nom, son prénom et le lieu et la date de sa naissance.

§ 2. L'entreprise concernée conserve la référence de l'opération de paiement et les données du formulaire en ligne ».

B.30.4. Étant donné que la disposition attaquée n'habilite les services de renseignement et de sécurité qu'à effectuer l'acte d'investigation attaqué « dans l'intérêt de l'exercice de leurs missions », ceux-ci doivent toujours disposer, à cet effet, d'indices concrets que l'identification de l'utilisateur final d'une carte de téléphonie mobile prépayée est nécessaire dans le cadre des missions énumérées limitativement à l'article 7 (Sûreté de l'État) et à l'article 11 (Service général du renseignement et de la sécurité) de la loi du 30 novembre 1998. Ces missions portant toutes sur des intérêts vitaux de la Nation, le fait de prendre une telle mesure suppose toujours au moins un risque que se produise un événement qui aurait des conséquences sociétales très graves.

B.30.5. La disposition attaquée garantit que la réquisition émane du dirigeant de service ou de son délégué et qu'elle est effectuée par écrit ou confirmée par écrit dans les 24 heures. Par ailleurs, l'article 16/2, § 4, de la loi du 30 novembre 1998 exige que les services de renseignement et de sécurité tiennent un registre de toutes les identifications requises. Ils doivent transmettre cette liste tous les mois au Comité permanent R.

À cet égard, les parties requérantes font valoir que la disposition attaquée n'exige pas que la réquisition du dirigeant de service ou de son délégué soit motivée. Cependant, une telle

obligation compromettrait le secret et l'efficacité des enquêtes menées par les services de renseignement et de sécurité.

B.30.6. La disposition attaquée ne garantit pas de contrôle judiciaire spécifique de la mesure d'enquête attaquée. Toutefois, comme il est dit en B.14.3, en matière de traitement et d'accès à de simples données d'identification, les voies de recours de droit commun suffisent (CEDH, 30 janvier 2020, *Breyer c. Allemagne*, § 106). À cet égard, l'intéressé dispose des voies de recours mentionnées en B.16.10.

B.30.7. Étant donné que l'acte d'investigation attaqué constitue une méthode ordinaire de collecte de données, la surveillance par la commission administrative visée à l'article 43/1 de la loi du 30 novembre 1998 et le contrôle *a posteriori* par le Comité permanent R visé aux articles 43/2 à 43/8 de la loi du 30 novembre 1998 n'y sont pas applicables.

Compte tenu de la portée limitée de la disposition attaquée, de l'intérêt fondamental de la sécurité nationale, du fait que la mesure attaquée ne permet aux services de renseignement et de sécurité que d'obtenir des données d'identification, et des garanties mentionnées en B.30.5, cette absence de surveillance ne suffit pas pour conclure que la disposition attaquée violerait le droit au respect de la vie privée.

B.30.8. Les parties requérantes font valoir en outre que, par les arrêts n^{os} 145/2011 du 22 septembre 2011 et 41/2019 du 14 mars 2019, la Cour a obligé le législateur à prévoir une obligation active de notification de la part des services de renseignement et de sécurité à quiconque a fait l'objet d'une enquête effectuée par ces services dès que le secret de l'enquête est levé.

Cependant, la Cour n'a imposé cette obligation qu'en ce qui concerne les méthodes exceptionnelles de collecte de données visées aux articles 18/12, 18/14 et 18/17 de la loi du 30 novembre 1998, qui permettent aux services de renseignement et de sécurité de prendre connaissance du contenu de communications. À cet égard, elle a considéré que ces méthodes étaient les plus intrusives dans la vie privée de l'intéressé. En revanche, elle n'a pas formulé cette exigence pour ce qui est des méthodes ordinaires de collecte de données ni des actes d'investigation qui portent seulement sur la collecte de données d'identification.

B.30.9. En ce que les parties requérantes font valoir enfin que la disposition attaquée permet aux services de renseignement et de sécurité de partager avec des services de renseignement et de sécurité étrangers les données d'identification recueillies, il suffit de constater qu'une telle collaboration ne fait pas l'objet de la disposition attaquée, mais de l'article 20 de la loi du 30 novembre 1998, qui n'est pas attaqué par les parties requérantes.

B.30.10. Sous réserve de l'interprétation mentionnée en B.30.4, le quatrième moyen n'est pas fondé.

Par ces motifs,

la Cour,

- annule l'article 2 de la loi du 1er septembre 2016 « portant modification de l'article 127 de la loi du 13 juin 2005 relative aux communications électroniques et de l'article 16/2 de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité », uniquement en ce qu'il ne détermine pas les données d'identification qui sont collectées et traitées et les documents d'identification qui entrent en considération;

- maintient les effets de la disposition annulée jusqu'à l'entrée en vigueur d'une norme législative qui énumère ces données d'identification et ces documents d'identification et au plus tard jusqu'au 31 décembre 2022 inclus;

- rejette le recours pour le surplus, sous réserve des interprétations mentionnées en B.8.7.3, B.16.6, B.16.8.5, B.16.8.7, B.26.2, B.26.6 et B.30.4.

Ainsi rendu en langue néerlandaise, en langue française et en langue allemande, conformément à l'article 65 de la loi spéciale du 6 janvier 1989 sur la Cour constitutionnelle, le 18 novembre 2021.

Le greffier, Le président,

P.-Y. Dutilleux L. Lavrysen